[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/20 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200680055229.9

[43] 公开日 2009 年 7 月 29 日

[11] 公开号 CN 101496024A

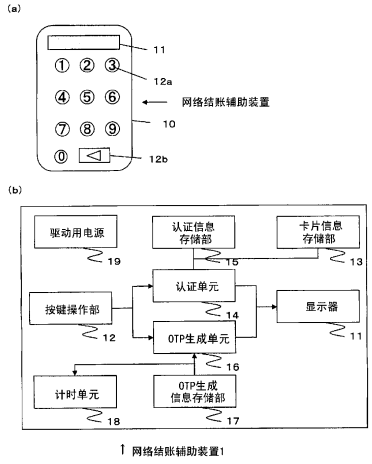
[22] 申请日 2006.7.10
[21] 申请号 200680055229.9
[30] 优先权
[32] 2006. 7. 7 [33] JP [31] 188341/2006
[86] 国际申请 PCT/JP2006/313658 2006.7.10
[87] 国际公布 WO2008/004312 日 2008.1.10
[85] 进入国家阶段日期 2009.1.4
[71] 申请人 株式会社吉世美
地址 日本东京
[72] 发明人 田中俊 川胜实之
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 张 鑫
权利要求书 3 页 说明书 33 页 附图 6 页

[54] 发明名称

网络结账辅助装置

[57] 摘要

本发明使卡号或密码被窃听、篡改的危险性消失，提供可更安全地进行网络商业交易的网络结账辅助装置。该网络结账辅助装置具备：显示器(11)；将卡片契约者的卡片信息以无法从外部读出的状态预先存储的卡片信息存储部(13)；将契约者的认证信息以无法从外部读出的状态预先存储的认证信息存储部(15)；将 OTP 生成信息以无法从外部读出的状态预先存储的 OTP 生成信息存储部(17)；数字键(12a)；根据来自数字键(12a)的输入信息将进行操作者本人认证的卡片信息显示于显示器(11)上的认证单元(14)；及在卡片信息被显示后根据 OTP 生成信息来生成一次性密码、并显示于显示器(11)的 OTP 生成单元(16)，通过一次性密码来进行契约者的本人认证，使得网络商业交易成为可行。



1 网络结账辅助装置1

1. 一种网络结账辅助装置，是可移动型的网络结账辅助装置，其特征在于，具有：

显示器；

卡片信息存储部，该卡片信息存储部以无法从外部读出的状态预先存储有至少包含信用卡或转帐卡等的卡片契约者的识别信息的卡片信息；

认证信息存储部，该认证信息存储部以无法从外部读出的状态预先存储有用来进行所述契约者的本人认证的认证信息；

OTP 生成信息存储部，该 OTP 生成信息存储部以无法从外部读出的状态预先存储有与所述卡片信息相关联且为所述网络结账辅助装置所固有的 OTP 生成信息；

输入单元，该输入单元将所述认证信息加以输入；

认证单元，该认证单元根据从所述输入单元所输入的输入信息，进行所述网络结账辅助装置的操作者是否为所述契约者的本人认证，已确认为本人时，至少读出所述卡片信息当中的所述识别信息，并显示于所述显示器上；及

一次性密码生成单元，该一次性密码生成单元在所述卡片信息被显示后，根据所述 OTP 生成信息生成一次性密码，并显示于所述显示器上，

当通过所述一次性密码进行所述契约者的本人认证、且已被确认为本人时，使得使用所述识别信息的结账的网络商业交易可行。

2. 一种网络结账辅助装置，是在信用卡或转帐卡等卡片契约者的手机或个人计算机等契约者终端和进行所述契约者本人认证的认证服务器彼此网络连接的网络结账系统中、在进行使用了所述契约者的识别信息的结账的网络商业交易时所被使用的可移动型的网络结账辅助装置，其特征在于，

所述网络结账辅助装置具有：

显示器；

卡片信息存储部，该卡片信息存储部以无法从外部读出的状态预先存储有至少包含所述契约者的识别信息的卡片信息；

认证信息存储部，该认证信息存储部以无法从外部读出的状态预先存储有

用来进行所述契约者的本人认证的认证信息；

OTP 生成信息存储部，该 OTP 生成信息存储部以无法从外部读出的状态预先存储有与所述卡片信息相关联且为所述网络结账辅助装置所固有的 OTP 生成信息；

输入单元，该输入单元将所述认证信息加以输入；

认证单元，该认证单元根据从所述输入单元所输入的输入信息，进行所述网络结账辅助装置的操作者是否为所述契约者的本人认证，已确认为本人时，至少读出所述卡片信息当中的所述识别信息，并显示于所述显示器上；及

一次性密码生成单元，该一次性密码生成单元在所述卡片信息被显示后，根据所述 OTP 生成信息生成一次性密码，并显示于所述显示器上，

所述契约者终端通过将所述一次性密码发送至所述认证服务器来进行所述契约者的本人认证，当已被确认为本人时，使所述网络商业交易可行。

3. 如权利要求 1 或 2 所述的网络结账辅助装置，其特征在于，

所述认证信息是所述契约者预先确定的密码；

所述输入单元是数字键。

4. 如权利要求 1 或 2 所述的网络结账辅助装置，其特征在于，

所述认证信息是将所述契约者的指纹、虹膜、声带、脸部照片等生物性特征加以数值化而成的生物信息。

5. 如权利要求 1 至 4 的任一项所述的网络结账辅助装置，其特征在于，

所述 OTP 生成信息是公共钥匙；

所述一次性密码生成单元中，

检测预定操作键的按下，将由所述操作键被按下时的日期时间构成的日期时间数据以所述公共钥匙予以加密来生成一次性密码。

6. 如权利要求 1 至 4 的任一项所述的网络结账辅助装置，其特征在于，

所述 OTP 生成信息由公共钥匙、和所述一次性密码每次被生成时就被更新的利用次数信息所构成；

所述一次性密码生成单元中，

检测预定操作键的按下，将所述利用次数信息以公共钥匙予以加密来生成一次性密码；

在所述一次性密码被生成后，将所述 OTP 生成信息存储部内的利用次数信息加以更新。

7. 如权利要求 1 至 6 的任一项所述的网络结账辅助装置，其特征在于，

所述网络结账辅助装置具有防篡改性。

网络结账辅助装置

技术领域

本发明涉及网络结账辅助装置。

背景技术

以往，在手机中预先存储有信用卡或银行卡等的卡片识别信息(卡号)及密码，当被输入至手机的密码和所存储的密码一致时，通过在手机的显示器上显示卡号，就可使手机也具备卡片的功能(例如，参照专利文献 1)。

可是，此种附带卡片功能的手机上，存在着以下说明的课题。

专利文献 1：日本国专利特开 2002-64597 号公报

对专利文献 1 所记载的附带卡片功能的手机的数据存储、消除等是通过通信进行的。换言之，该手机是以被网络连接为前提的。

如此，若在可连接网络的手机中预先存储卡号或密码，则因不正当访问等，这些卡号或密码被恶意第三者窃听、篡改的危险性大，会造成安全上的问题。

于是，若将手机构成为不可连接网络的话，则或许可以使上述窃听或篡改的疑虑消失。

可是，目前手机除了基本的通话功能以外，一般还具有网络通信功能，要使手机变成不可连接网络的构成，这在现实上是有困难的。又，为了要维持现状的手机的构成不变，且使已被存储的卡号或密码无法从外部读出，需要具备加密程序等，会使构成变得复杂。

又，在专利文献 1 的手机的情况中，即使不通过上述的通过网络的不正当访问，只要显示在手机的显示器上的卡号被第三者偷看到一次，则第三者便能使用该卡号，在因特网上进行信用结账的网络商业交易，就这点来说，安全性亦较低。

此外，本案专利申请人鉴于上述这种仅用卡号就可进行网络商业交易的情

况，而正在开始运用一种除了卡号的提示外，还须经过提示持卡会员所预先确定的固定密码来进行持卡会员的本人认证，才能进行网络商业交易的这种网络结账系统。

可是，若该固定密码也一旦被第三者得知，则第三者还是可假冒持卡会员来进行网络商业交易，也未必能够说是安全的。

发明内容

本发明是鉴于以上的现有问题而研发的，其目的在于提供一种使得不正当访问等造成卡号或密码被窃听、篡改的危险性消失，且能够更安全地进行网络商业交易的网络结账辅助装置。

权利要求 1 的发明，是

一种网络结账辅助装置，是可移动型的网络结账辅助装置，其中，具备：显示器；卡片信息存储部，该卡片信息存储部以无法从外部读出的状态预先存储有至少包含信用卡或转帐卡等的卡片契约者的识别信息的卡片信息；认证信息存储部，该认证信息存储部以无法从外部读出的状态预先存储有用来进行所述契约者的本人认证的认证信息；OTP(One Time Password：一次性密码)生成信息存储部，该 OTP 生成信息存储部以无法从外部读出的状态预先存储有与所述卡片信息相关联且为所述网络结账辅助装置所固有的 OTP 生成信息；输入单元，该输入单元将所述认证信息加以输入；认证单元，该认证单元根据从所述输入单元所输入的输入信息，进行所述网络结账辅助装置的操作者是否为所述契约者的本人认证，已确认为本人时，至少读出所述卡片信息当中的所述识别信息，并显示于所述显示器上；及一次性密码生成单元，该一次性密码生成单元在所述卡片信息被显示后，根据所述 OTP 生成信息，生成一次性密码，并显示于所述显示器上；当通过所述一次性密码，进行了所述契约者的本人认证，且已确认为本人时，使得使用所述识别信息的结账的网络商业交易成为可行。

权利要求 2 的发明，是

一种网络结账辅助装置，是在信用卡或转帐卡等卡片契约者的手机或个人计算机等契约者终端、和进行所述契约者本人认证的认证服务器彼此网络连接

的网络结账系统中，在进行使用了所述契约者的识别信息的结账的网络商业交易时所被使用的可移动型的网络结账辅助装置，其中，所述网络结账辅助装置具备：显示器；卡片信息存储部，该卡片信息存储部以无法从外部读出的状态预先存储有至少包含所述契约者的识别信息的卡片信息；认证信息存储部，该认证信息存储部以无法从外部读出的状态预先存储有用来进行所述契约者的本人认证的认证信息；OTP 生成信息存储部，该 OTP 生成信息存储部以无法从外部读出的状态预先存储有与所述卡片信息相关联且为所述网络结账辅助装置所固有的 OTP 生成信息；输入单元，该输入单元将所述认证信息加以输入；认证单元，该认证单元根据从所述输入单元所输入的输入信息，进行所述网络结账辅助装置的操作者是否为所述契约者的本人认证，已确认为本人时，至少读出所述卡片信息当中的所述识别信息，并显示于所述显示器上；及一次性密码生成单元，该一次性密码生成单元在所述卡片信息被显示后，根据所述 OTP 生成信息，生成一次性密码，并显示于所述显示器上；所述契约者终端通过将所述一次性密码发送至所述认证服务器来进行所述契约者的本人认证，当已确认为本人时，使所述网络商业交易成为可行。

根据权利要求 1 及权利要求 2 的发明，则若利用网络结账辅助装置进行契约者的本人认证的结果，未确认为本人的话，则由于即使是契约者自身也无法获知卡片信息，而卡片信息是以无法从外部读出的状态而被存储的，因此，与卡片信息会泄漏的现有的信用卡不同，可提高卡片信息的隐匿性，防止网络商业交易中的卡片信息的不正当使用。

又，由于网络结账辅助装置为可移动型，因此无论契约者身处何处，都可使用手机、家中的个人计算机、外出地的个人计算机，来进行安全的网络商业交易，增加网络商业交易的便利性。

又，因为契约者的本人认证时，是使用根据网络结账辅助装置中所存储的契约者固有的 OTP 生成信息而生成的一次性密码，因此，即使第三者获得一次性密码，也不能在下次的网络商业交易中使用。

一次性密码生成用的 OTP 生成信息，因为是以无法从外部读出的状态而被存储的，因此即使是契约者本人，也无从得知 OTP 生成信息，只有正在操作网络结账辅助装置的契约者本人才能获知生成结果的一次性密码。换言之，

由于不可能由第三者来生成一次性密码，因此，更加保证网络商业交易的安全性。

而且，该一次性密码的生成，是只有在网络结账辅助装置上显示了卡片信息后才会进行的，因此，不具有网络结账辅助装置的第三者，即使只是知道识别信息，也无法生成一次性密码。又，即使第三者窃得了网络结账辅助装置，若没有输入到网络结账辅助装置的认证信息，也无法生成一次性密码。

换言之，契约者在利用网络结账辅助装置的认证单元接受了本人认证后，还要利用认证服务器接受本人认证，通过这样在一直到最终可进行网络商业交易之前必须要经过根据 2 种不同的认证信息的本人认证，因此能更好地防止第三者的假冒，提高网络商业交易的安全性。

权利要求 3 的发明，是

一种网络结账辅助装置，其中，所述认证信息是所述契约者所预先确定的密码，所述输入单元是数字键。

根据权利要求 3 的发明，由于可使输入单元及认证单元构成较为廉价，因此可谋求促进网络结账辅助装置的利用。

权利要求 4 的发明，是

一种网络结账辅助装置，其中，所述认证信息是将所述契约者的指纹、虹膜、声带、脸部照片等生物性特征加以数值化而成的生物信息。

根据权利要求 4 的发明，因为能以高精度来进行契约者的本人认证，因此可成为即使网络结账辅助装置遭窃、也不必担心遭到滥用的网络结账辅助装置。

权利要求 5 的发明，是

一种网络结账辅助装置，其中，所述 OTP 生成信息是公共钥匙；所述一次性密码生成单元检测预定操作键的按下，而将由所述操作键被按下的日期时间构成的日期时间数据以所述公共钥匙予以加密来生成一次性密码。

权利要求 6 的发明，是

一种网络结账辅助装置，其中，所述 OTP 生成信息由公共钥匙，和所述一次性密码每次被生成时就被更新的利用次数信息所构成；所述一次性密码生成单元，检测预定操作键的按下，而将所述利用次数信息以公共钥匙予以加密

来生成一次性密码；在所述一次性密码被生成后，将所述 OTP 生成信息存储部内的利用次数信息加以更新。

此处所生成的一次性密码使用公共钥匙，将由预定按键被按下的日期时间构成的日期时间数据或者每次生成一次性密码时就会被更新的利用次数信息予以加密而成。即，由于是只有正在操作网络结账辅助装置的契约者才能生成的密码，因此不持有网络结账辅助装置的第三者无法假冒契约者来进行网络商业交易，可进一步提升网络商业交易的安全性。

权利要求 7 的发明，是

一种网络结账辅助装置，其中，所述网络结账辅助装置具备防篡改性(Tamper Proofness)。

根据权利要求 7 的发明，由于网络结账辅助装置具备防篡改性，故可谋求进一步提升对由第三者所致的卡片信息、认证信息、OTP 生成信息的窃听、篡改的安全性提升。

根据本发明的网络结账辅助装置，若通过网络结账辅助装置进行契约者的本人认证的结果是未确认为本人的话，则由于即使是契约者自身也无法获知卡片信息，而卡片信息是以无法从外部读出的状态而被存储，因此，与卡片信息会泄漏的现有的信用卡不同，可提高卡片信息的隐匿性，防止网络商业交易中的卡片信息的不正当使用。

又，由于网络结账辅助装置为可移动型，因此无论契约者身处何处，都可使用手机、家中的个人计算机、外出地的个人计算机，来进行安全的网络商业交易，增加网络商业交易的便利性。

又，因为契约者的本人认证时，是使用根据网络结账辅助装置中所存储的契约者固有的 OTP 生成信息而生成的一次性密码，因此，即使第三者获得一次性密码，也不能在下次的网络商业交易中使用。

一次性密码生成用的 OTP 生成信息，因为是以无法从外部读出的状态而被存储，因此即使是契约者本人，也无从得知 OTP 生成信息，只有正在操作网络结账辅助装置的契约者本人才能获知生成结果的一次性密码。换言之，由于不可能由第三者生成一次性密码，因此，可更加保证网络商业交易的安全性。

而且，该一次性密码的生成，是只有在网络结账辅助装置上显示了卡片信息后才会进行，因此，不具有网络结账辅助装置的第三者，即使只是知道识别信息，也是不能生成一次性密码的。又，即使第三者窃得了网络结账辅助装置，若没有输入到网络结账辅助装置的认证信息，也无法生成一次性密码。

换言之，契约者在通过网络结账辅助装置的认证单元接受了本人认证后，还会通过认证服务器而接受本人认证，由于一直到最终可进行网络商业交易为止必须要经过根据 2 种不同的认证信息的本人认证，因此能更加防止第三者所致的假冒，提高网络商业交易的安全性。

附图说明

图 1 是本发明的网络结账辅助装置的外观及电气硬件构成的构成图。

图 2 是使用网络结账辅助装置的网络结账系统的概要连接构成图。

图 3 是网络结账系统中的网络商业交易的处理流程的一个例子的图。

图 4 是网络结账系统中的网络商业交易的处理流程中，显示于会员终端的画面的一个例子的图。

图 5 是表示网络结账辅助装置的操作程序及显示器画面转移的图。

图 6 是未使用网络结账辅助装置的网络结账系统被持卡会员利用时，为注册用于持卡会员的本人认证的密码所需的系统概要连接构成图。

标号说明

1：网络结账辅助装置

10：外壳

11：显示器

12：按键操作部

12a：数字键

12b：开始键

13：卡片信息存储部

14：认证单元

15：认证信息存储部

16：OTP 生成单元

17：OTP 生成信息存储部

18：计时单元

19：驱动用电源

2：会员终端

3：加盟店终端

4：收单银行终端

5：中介服务器

6：发卡银行终端

7：认证服务器

9a：网络

9b：专线

具体实施方式

以下，针对本发明的理想实施方式，根据附图来详细说明。图 1(a)是网络结账辅助装置 1 的外观图，图 1(b)是网络结账辅助装置 1 的电气硬件的构成图。

网络结账辅助装置 1 是在信用卡或转帐卡等的卡片契约者的契约者终端(手机或个人计算机等)，和进行契约者本人认证的认证服务器(通常是由持卡会员所保有)彼此网络连接而成的网络结账系统中，当契约者使用该契约者的识别信息来进行结账，以进行网络购物等网络商业交易时所被使用的；如图 1(a)所示，具有可收容于手掌程度的外形，由薄型且可手持搬运的外壳 10 所构成，在外壳 10 的外表面上，外露出显示器 11、和按键操作部 12。

此外，本实施例的显示器 11 是 8 位数显示的显示器；按键操作部 12 由 0～9 的数字键 12a、和开始键 12b 所构成。

外壳 10 的内部如图 1(b)所示，除了显示器 11、按键操作部 12 以外，还有用来作为卡片信息存储部 13、认证信息存储部 15、认证单元 14、OTP 生成单元 16、OTP 生成信息存储部 17、计时单元 18 而起到各自功能的硬件(CPU、内存)，和用来驱动这些硬件电气器件(显示器 11、按键操作部 12、CPU、内存)的驱动用电源 19(电池)所构成。

此外，本实施例的外壳 11 中，除了显示器 11 和按键操作部 12 的驱动用电源 19 以外，还设有内置 SIM 等 IC 卡的插槽，在该插槽中插入 IC 卡来使用。然后，上述 CPU 和内存使用该 IC 卡中含有的内容。如后述，由于卡片信息存储部 13、认证信息存储部 15、OTP 生成信息存储部 17 中存储着每位契约者不同的信息，因此，将此类信息存储在 IC 卡的内存中，插入插槽而使用，藉此，外壳 10 自身与契约者无关是公共的，且外壳 10 自身不保有个人信息，因此，可提升外壳 10 的生产性，并且可使外壳 10 的取用、管理较为容易。

又，本实施例的驱动用电源 19 虽然为钮扣型电池，但亦可为太阳能电池或充电电池等。又，网络结账辅助装置 1 还可设计成，在通常时保持电源断开状态，而在例如当按键操作部 12 的任一键被操作时，才启动电源。

本实施例的卡片信息存储部 13、认证信息存储部 15、OTP 生成信息存储部 17，具体而言，是由分别存储有后述的卡片信息、认证信息、OTP 生成信息的内存所构成的；内存在物理上可为将这些信息综合存储的 1 个内存，亦可为 2 个以上的内存。

本实施例的认证单元 14 及 OTP 生成单元 16，具体而言，是由被存储在内存中的程序所构成的；网络结账辅助装置 1 内的 CPU 通过从内存中读出该程序并执行，以实现这些认证单元 14 及 OTP 生成单元 16 的功能。此外，在不具备 CPU、内存的网络结账辅助装置上，认证单元 14、OTP 生成单元 16 的功能，亦可使用电子器件以电路方式来加以实现。

本实施例的网络结账辅助装置 1，是从根据与信用卡组织(credit card brand)的授权契约而发行信用卡的发卡银行(若为转帐卡，则是发行转帐卡的银行或者卡片发行公司)来对每一位持卡会员也就是契约者，在发卡银行中以每位契约者所固有的卡片信息、认证信息、OTP 生成信息被存储在内存中的状态下，所发放出来的(发放的形态可为借贷、转让)；且被构成为，在发放后，内存（卡片信息存储部 13、认证信息存储部 15、OTP 生成信息存储部 17）的存储内容无法从外部读出。

又，即使是被发放网络结账辅助装置 1 的契约者自身，也无法从外部读出内存的存储内容。契约者自身只有在进行契约者的本人认证、且被确认为本人时，才能通过卡片信息被显示在显示器 11 上，而仅能得知该卡片信息，除此

以外的状态下，卡片信息是被隐匿化。

之所以设计成不让内存的存储内容可从外部读出的理由，是因为网络结账辅助装置 1 不具备连接因特网等的网络的接口，是属于非网络连接型的终端。

此外，为了进一步提升对内存存储内容的窃听、篡改的安全性，网络结账辅助装置 1、或内置于网络结账辅助装置 1 的 SIM 等 IC 卡，还可具备防篡改性(若试图分解、或从内存直接读取内容，则内存的存储内容会被抹除、或是程序变成无法启动的性质)。

以下，针对网络结账辅助装置 1 的各部细节加以说明。

卡片信息存储部 13，是将至少包含契约者的识别信息的卡片信息，以无法从外部读出的状态预先存储而成的内存；本实施例的卡片信息由契约者固有的识别信息(卡号)、有效期限、和安全码(以预定的方法预先加密过的 3 位数的 10 进制数。通常在塑料型的信用卡的签名板上有被印出。通过该数字，就可确认该卡片的真正性)所构成。又，亦可包含名义人名。又，卡片信息亦可仅单纯由识别信息来构成。又，卡片信息无需包含有效期限、安全码、名义人名的全部，亦可适当地组合 1 者以上来构成卡片信息。

认证信息存储部 15，是将契约者所确定的密码，或将契约者的指纹、虹膜、声带、脸部照片等的生物性特征予以数值化而成的生物信息等进行契约者本人认证所需的认证信息以无法从外部读出的状态，预先存储的内存。

此外，认证信息存储部 15 中所存储的认证信息，与网络结账系统中的认证服务器在契约者本人认证时所用的认证信息不同，是网络结账辅助装置 1 为了进行契约者本人认证所需的认证信息。又，认证服务器中的认证信息和网络结账辅助装置 1 中的认证信息其种类不同。

OTP 生成信息存储部 17，是将网络结账辅助装置 1 所固有的 OTP 生成信息以无法从外部读出的状态而预先存储的内存；本实施例的 OTP 生成信息是网络结账辅助装置 1 上所固有的公共钥匙；公共钥匙，是在进行由 OTP 生成单元 16 所生成的一次性密码的验证的服务器(后述的实施例中的认证服务器)中，与存储在卡片信息存储部 13 的识别信息相关联。

此外，公共钥匙，是在网络商业交易中只会被存储在进行契约者本人认证的认证服务器、和网络结账辅助装置 1 的钥匙；在本实施例中，后述的 OTP

生成单元 16，在生成一次性密码时会使用到。

认证单元 14，是为用来进行确认网络结账辅助装置 1 的操作者，是否为可利用卡片信息存储部 13 中所存储的识别信息的契约者(持卡会员)的本人认证的单元；是确认从输入单元(本实施例中为数字键 12a)所输入的输入信息，和认证信息存储部 15 中所存储的认证信息是否一致，当为一致时，则视为网络结账辅助装置 1 的操作者为该契约者本人，而至少将卡片信息存储部 13 中所存储的卡片信息当中的识别信息予以读出，并显示于显示器 11 上的单元。

本实施例的认证单元 14 通过操作者按下按键操作部 12 的开始键 12b，就接受开始键 12b 的按下检测而开始启动。然后，一旦操作者按下了相当于输入单元的数字键 12a 而输入 4 位数的数字时，则认证单元 14 确认所输入的数字和认证信息存储部 15 中所存储的密码是否一致，若为一致，则在显示器 11 上显示出卡片信息。

认证信息若像本实施例是密码，则作为输入单元只要为数字键即可，输入信息和认证信息的一致判断处理也可容易进行，可以较廉价的构成来实现网络结账装置 1，可谋求促进网络结账装置 1 的利用。

本实施例的认证信息虽然是 4 位数的密码，但认证方法及认证信息并非局限于此，亦可适当地组合多种认证方法的认证单元，若采用多个认证单元，则其可换来认证精度的提高，可防止第三者所致的网络结账辅助装置的滥用。

例如，认证单元 14 若采用生物计量认证方法，则认证信息为生物计量信息(将指纹、虹膜、声带、脸部照片等的生物性特征予以数值化而成的数据)，又，输入单元是改为用来输入这些生物计量信息的扫描仪、麦克风、数字摄像机等。

由于生物计量认证方法是高精度的认证方法，因此即使网络结账辅助装置 1 被第三者窃取，只要不是身为网络结账辅助装置 1 所被发放的契约者，就无法使用网络结账辅助装置 1，而可防止遭到滥用。

又，作为本实施例的认证信息的密码中，除了数字以外，还可含有英文字母；此时，除了数字键以外，网络结账辅助装置还需要具有英文字母键。

OTP 生成单元 16，是在通过认证单元 14 而显示出卡片信息后，根据 OTP 生成信息存储部 17 中所存储的 OTP 生成信息(本实施例中为公共钥匙)，来生

成一次性密码，并显示于显示器 11 上的单元。

该一次性密码是从契约者终端被发送至认证服务器，并由认证服务器进行契约者本人认证时，与在认证服务器上根据 OTP 生成信息所生成的一次性密码进行核对时所使用的。然后，当这些一次性密码的核对结果为一致，而被认证服务器确认为本人时，使用该契约者的识别信息的结账的网络商业交易就变成可行。

本实施例中，在进行认证单元 14 的认证且卡片信息被显示于显示器 11 上后，一旦操作者按下开始键 12b，则开始键 12b 被按下即成为令 OTP 生成单元启动的契机，而会生成、显示一次性密码。

此外，本实施例的 OTP 生成单元 16，虽然是由详细后述的时间同步方式来生成一次性密码，但亦可为其它的生成方式，例如：计数器同步方式、或询问&响应方式，来生成一次性密码。

计时单元 18，是为本实施例的 OTP 生成单元 16 以时间同步方式生成一次性密码时所需的单元，是计时的单元。此外，计时单元 18 可由实时时钟来构成，或可将计时程序存储于内存，由 CPU 将该计时程序读出并执行而实现计时功能的方式。又，OTP 生成单元 16 在以时间同步方式以外的方式来生成一次性密码时，不需要计时单元 18，取而代之而添加各生成方式所需的单元。

本实施例中，OTP 生成单元 16 如上所述，认证单元 14 接受在显示器 11 上显示的卡片信息，而成为开始键 12b 的按下检测等待状态。OTP 生成单元 16，一旦检测出开始键 12b 的按下，则将检测出按下的事件传达给计时单元 18。计时单元 18，对开始键 12b 被测出按下的日期时间进行计时，将日期时间数据(年月日时分秒。秒是以 30 秒为单位)交付给 OTP 生成单元 16。

然后，OTP 生成单元 16 从 OTP 生成信息存储部 17 读出公共钥匙，将所被交付的日期时间数据以读出的公共钥匙予以加密，将其转换成十进制数，显示于显示器 11。此外，本实施例的加密方式，虽然是采用公共钥匙加密方式，但亦可用其它的加密方式。

根据以上说明的网络结账辅助装置 1，通过网络结账辅助装置 1 来进行契约者的本人认证，并确认为本人时，认证单元 14 所显示的卡片信息被输入至从可进行卡片结账的加盟店的网站或认证服务器所发送过来的显示于契约者

终端上的卡片信息输入画面后，就可被发送至网站或认证服务器。

如此，若通过网络结账辅助装置 1，进行契约者的本人认证而确认为本人，即，若所输入的输入信息与网络结账辅助装置中所存储的认证信息一致，则由于即使是契约者自身也无法获知卡片信息，而卡片信息是以无法从外部读出的状态而被存储发热，因此，与卡片信息会泄漏的现有的信用卡不同，可提高卡片信息的隐匿性，防止网络商业交易中的卡片信息的不正当使用。

又，由于网络结账辅助装置是可移动型，因此无论契约者身处何处，都可使用手机、家中的个人计算机、外出地的个人计算机，来进行安全的网络商业交易，增加网络商业交易的便利性。

又，OTP 生成单元 16 所显示的一次性密码在被输入至从进行契约者的本人认证的认证服务器所发送过来的显示于契约者终端的一次性密码输入画面后，可被发送至认证服务器，并且通过与认证服务器所生成的一次性密码的核对，当为一致时，则确认为本人，使用契约者识别信息的结算的网络商业交易就变成可行。

如此，因为契约者的本人认证时，是使用根据网络结账辅助装置中所存储的契约者固有的 OTP 生成信息而生成的一次性密码，因此，即使第三者获得一次性密码，也不能使用在下次的网络商业交易中。

一次性密码生成用的 OTP 生成信息，因为是以无法从外部读出的状态而被存储，因此即使是契约者本人，也无从得知 OTP 生成信息，只有正在操作网络结账辅助装置的契约者本人才能获知生成结果的一次性密码。换言之，由于第三者所致的一次性密码生成是不可能发生，因此，可更加保证网络商业交易的安全性。

而且，该一次性密码的生成，是只有在网络结账辅助装置上显示了卡片信息后才会进行，因此，不具有网络结账辅助装置的第三者，即使只是知道识别信息，也是不能生成一次性密码。又，即使第三者窃得了网络结账辅助装置，若没有输入至网络结账辅助装置的认证信息，也是无法生成一次性密码。

换言之，契约者在通过网络结账辅助装置的认证单元接受了本人认证后，还会通过认证服务器而接受本人认证，通过这样一直到最终可进行网络商业交易为止是需要经过根据 2 种不同的认证信息的本人认证，因此能更加防止第三

者所致的假冒，提高网络商业交易的安全性。

此外，认证信息存储部 15 亦可设计成，除了上述认证信息以外，还可在认证单元 14 所进行的一致判定处理中，发现输入信息和认证信息并不一致时，预先存储有可接受输入信息重新输入的次数(错误容许次数)。此时，网络结账辅助装置 1 或认证单元 14 其构成为也要具备计数单元(计数器)。

然后，在认证单元 14 进行一致判定处理的流程中，当输入信息和认证信息不一致时，则每次在其发生时，计数单元就会从 1 起往上计数，并比较被往上计数后的数字与错误容许次数，当往上计数后的数字超过了错误容许次数时，以后就使认证单元 14 不进行自身的处理，并且也使 OTP 生成单元 16 不启动，以使认证流程及 OTP 生成流程不被进行。

藉此，就可防止恶意第三者盗用网络结账辅助装置 1 来处理认证信息然后输入，结果导致卡片信息或一次性密码被显示在显示器 11 上。

此外，当往上计数后的数字没有超过错误容许次数，而输入信息和认证信息一致时，认证单元 14 会在显示器 11 上进行卡片信息的显示，而此时被计数的数字，会被重置(初始化)变成 0。

此处，将网络结账辅助装置 1 的操作程序及显示器 11 的画面转移的一例，示于图 5。此外，本实施例的显示器 11，是为 8 位数的英数字・记号显示用显示器。

首先，一旦开始键 12b 被操作者按下，则网络结账辅助装置 1 的电源便启动(S200)，在显示器 11 上会显示「APPLI」(S210)，因此当想在开始键 12b 被按下后(S225)还要显示卡片信息时，操作者按下数字键 12a 的「1」(S230)；当想要进行认证信息(密码)的变更时，则按下数字键 12a 的「2」(S330)。

由于当「1」被按下的时候(S230)，显示器 11 上会显示「PIN」，所以操作者是将作为认证信息的 4 位数密码，从数字键 12a 中选择出来并按下(S240)。其后，开始键 12b 被按下(S245)，已按下的密码，若和认证信息存储部 15 中所存储的认证信息一致，则将卡片信息存储部 13 中所存储的卡片信息当中，首先将识别信息(以下称为卡号)的前 8 位数，显示于显示器 11(S250)。

接着，一旦开始键 12b 被按下(S255)，则卡号的后 8 位数会被显示在显示器 11 上(S260)。

接着，一旦开始键 12b 被按下(S265)，则有效期限和安全码会被显示在显示器 11 上(S270)。此外，S265 和 S270 的流程并非必须，亦可仅显示出卡片信息当中的卡号。

接着，一旦开始键 12b 被按下(S275)，则显示器 11 会显示「OTP＝1」，而进行要生成、显示一次性密码，或是否结束的选择。此处，在开始键 12b 被按下后(S290)，再按下数字键 12a 的「1」(S295)，则显示器 11 上会显示催促认证信息的输入的「PIN」(S305)，因此，操作者再度从数字键 12a 按下 4 位数的密码，并按下开始键 12b(S310)。

已按下的密码，若和认证信息存储部 15 中所存储的认证信息一致，则根据 OTP 生成信息存储部 17 中所存储的 OTP 生成信息，生成一次性密码，并将其显示在显示器 11 上(S315)。

然后若开始键 12b 再次被按下(S320)，则网络结账辅助装置 1 的电源就被切断。

当数字键 12a 的「1」以外的键被按下，或任一键都没被按下、经过了预先决定的预定时间后(S300)，则网络结账辅助装置 1 会自动地切断电源。

此外，S240 和 S305 中所输入的密码亦可为卡片信息显示用和一次性密码生成用中不同的密码，此时，认证信息存储部 15 中，将各个密码予以区别而存储。

又，本实施例中，虽然是在一次性密码显示于显示器 11 的流程(S315)之前，以 S305 再度向操作者催促输入认证信息，但是，亦可设计成省略 S305，仅须 S310 的开始键 12b 按下，就可生成一次性密码。

S225 之后，若数字键 12a 的「2」被按下(S330)，则显示器 11 上会显示「CHANGE？」(S335)。

一旦开始键 12b 被按下(S340)，则在显示器 11 上会显示「PIN」，催促密码的输入，因此，操作者从数字键 12a 按下 4 位数的密码后(S345)，再按下开始键 12b(S350)，若已被按下的密码，与认证信息存储部 15 中所存储的认证信息一致，则用来催促变更后的密码输入的「NEW1」会显示于显示器 11 上，因此，操作者是从数字键 12a 按下变更后的密码(S355)，然后再按下开始键 12b(S360)。

其次，因为在显示器 11 上会显示用来催促再次输入变更后密码的「NEW2」，因此操作者要再度从数字键 12a 按下变更后的密码(S365)，然后按下开始键 12b(S370)。

若 S355 中被按下的密码，和 S365 中所按下的密码一致，则显示器 11 上会显示旨在表示密码变更已完成的「COMPLETE」(S375)，因此一旦在经过确认后，开始键 12b 被按下(S380)，则密码的变更程序就完成，电源会被切断。

此外，为了提升安全性，S355 和 S365 中，即使有从数字键 12a 进行输入，所输入的值也不会被显示在显示器 11 上较为理想。

实施例 1

以下，针对被发放了图 1 所示的网络结账辅助装置 1 的信用卡契约者也就是信用卡会员(以下称为持卡会员)使用网络结账辅助装置 1，由具有通信功能的个人计算机或手机，通过使用该持卡会员的卡号的结账，来进行网络购物等网络商业交易(以下称为网络商业交易)时的一实施例，加以说明。

本实施例的网络结账系统的系统构成和网络连接关系，示于图 2 的系统构成图。又，本实施例的网络结账系统中的网络商业交易的流程，示于图 3 的流程图。

此外，本实施例中，网络结账系统中提供网络商业交易服务的是信用卡组织(credit card brand)。

持卡会员预先对发卡银行进行信用卡的申办，接受信用卡的发行，并且还从发卡银行，接受存储有每位持卡会员所固有的认证信息(持卡会员在申办信用卡时所注册的密码或指纹信息等生物信息)、卡片信息(每位持卡会员所固有的卡号、有效期限)、OTP 生成信息(公共钥匙)的网络结账辅助装置 1 的发放。

又，本实施例中，虽然图 1(b)所示的网络结账辅助装置 1 的构成当中，除了显示器 11 和按键操作部 12 和驱动用电源 19 的构成，是预先存储在 SIM 等 IC 卡中，并通过在设于外壳 10 的 IC 卡插槽(未图示)中插入该 IC 卡，来实现网络结账辅助装置 1 的功能，但是，网络结账辅助装置并非一定要具备 IC 卡，当不具备 IC 卡时，只要网络结账辅助装置自身具备 CPU 或内存即可。

又，本实施例的网络结账辅助装置 1，虽然是在利用了使用持卡会员识别

信息的结账、即卡片结账的网络商业交易中所被使用的，但当持卡会员只希望进行网络商业交易，不希望先前的由塑料型磁卡、IC 卡等所构成的信用卡所致的真实的面对面交易的情况下，亦可不接受信用卡的发行。

又，当信用卡组织，也有进行发卡银行的业务的情况下，亦可从信用卡组织来发放网络结账辅助装置 1。

会员终端 2 是契约者的终端，是持卡会员使用网络结账辅助装置 1 进行网络商业交易所需的终端，是至少具有通信功能和浏览显示功能的个人计算机、手机等终端。

加盟店终端 3 是向会员终端 2 提供虚拟店铺(网站)，接受商品或服务的订购，并且向发卡银行侧委托已订购的持卡会员的本人认证，在进行过持卡会员的本人认证后，对收单银行(根据与信用卡组织的授权契约，进行加盟店的获得・契约・管理业务等)，委托进行授权(调查所订购的商品或服务的金额量的信用额度在持卡会员身上是否还有剩余，若有剩余信用额度则将该金额量确保成结账用)的终端。

收单银行终端 4，是为将从加盟店终端 3 所受取的授权委托，再委托给发卡银行侧(授权再转送)的终端。

中介服务器 5 担任加盟店终端 3 和后述的认证服务器 7 的中介，即，是在会员终端 2 和加盟店终端 3 之间，担任持卡会员的认证服务的中介角色的服务器。

中介服务器 5，在本实施例中是信用卡组织所营运的服务器，存储有用来识别使用网络结账辅助装置 1 的网络商业交易服务所对应的加盟店的加盟店识别信息，和用来识别使用网络结账辅助装置 1 的网络商业交易服务所对应的发卡银行的发卡银行识别信息。

此外，本实施例的网络结账系统中，当混合有不使用网络结账辅助装置 1 的网络商业交易服务存在时，则中介服务器 5，需要将不支持使用网络结账辅助装置 1 的商业交易服务的加盟店及发卡银行的识别信息、和上述加盟店识别信息及发卡银行识别信息加以区别而存储。

发卡银行终端 6，是为接受从收单银行终端 4 收到的授权委托，进行授权的终端。

认证服务器 7，是在进行网络商业交易时，早于授权，先进行持卡会员本人认证的服务器。本实施例中，认证服务器 7，是发卡银行所营运的服务器，与发卡银行终端 6 连接，并且是将可能进行使用网络结账辅助装置 1 的网络商业交易的持卡会员的卡片信息(卡号、有效期限)及 OTP 生成信息(网络结账辅助装置 1 所固有的公共钥匙)，以彼此相关联的状态，加以存储。换言之，每 1 持卡会员，都与卡片信息和 OTP 生成信息相关联，而被存储在认证服务器 7 中。

此外，往认证服务器 7 的这些信息的存储，是在向持卡会员发放网络结账辅助装置 1 的同时期，或其前后进行的。

图 2 中，会员终端 2、加盟店终端 3、中介服务器 5、认证服务器 7 间，分别通过因特网等网络 9a 而连接；加盟店终端 3、收单银行终端 4、发卡银行终端 6，分别通过专线 9b 而连接。

此外，发卡银行终端 6 及认证服务器 7，是对每个发卡银行个别准备的，分别与会员终端 2、收单银行终端 4、中介服务器 5，以网络 9a、专线 9b 而连接。

又，加盟店终端 3 也是对每个加盟店个别准备的，分别与会员终端 2、中介服务器 5、收单银行终端 4，以网络 9a、专线 9b 而连接。

以下，根据图 3 的流程图及图 2 的系统构成图，说明使用网络结账辅助装置 1 的网络商业交易的流程。持卡会员从会员终端 2，通过网络 9a，访问作为虚拟店铺(Web 网站)的加盟店终端 3，并阅览商品或服务。然后，一旦决定了要订购的商品或希望的服务，则会员终端 2 向加盟店终端 3 发送关于订购商品或希望服务的、希望用卡片结账的网络商业交易的意向。

加盟店终端 3 使会员终端 2 显示如图 4(a)所示的卡片信息输入画面 100，并向会员终端 2 请求输入并发送卡号及卡片的有效期限。

于是，一旦持卡会员按下了网络结账辅助装置 1 的开始键 12b，则网络结账辅助装置 1 的认证单元 14 便启动，网络结账辅助装置 1 成为等待认证的状态。接下来，持卡会员将本人认证所必须的输入信息(本实施例中为 4 位数的密码)从数字键 12a 进行输入。此外，此处所输入的 4 位数的密码，是预先在持卡会员申办卡片时就已经决定的，且已经被存储在网络结账辅助装置 1 内的认

证信息存储部 15 中。

认证单元 14 将认证信息存储部 15 中所存储的认证信息加以读出，并确认是否和从数字键 12a 所输入的输入信息一致。然后，当两者为一致时，认证单元 14 从卡片信息存储部 13 读出作为卡片信息的卡号和有效期限，并显示于显示器 11 上。

然后，若卡号和有效期限全部在显示器 11 上显示完毕，则认证单元 14 将显示完毕的情况传达给 OTP 生成单元 16。藉此，OTP 生成单元 16 成为后述的一次性密码生成等待状态。

此外，本实施例中，由于显示器 11 所能显示的位数限制为 8 位数，因此认证单元 14 先将从卡片信息存储部 13 读出的卡号进行分割处理而分成前 8 位和后 8 位，然后在显示器 11 上先显示卡号的前 8 位。持卡会员根据该显示，在卡片信息输入画面 100 的卡号输入栏 100a 中输入卡号的前 8 位数。

一旦卡号的前 8 位数的输入结束，则持卡会员按下开始键 12b。认证单元 14 接受开始键 12b 的按下检测，而将卡号的后 8 位数显示于显示器 11 上。持卡会员根据该显示，在卡片信息输入画面 100 的卡号输入栏 100a 中输入卡号的后 8 位数。

一旦卡号的后 8 位数的输入结束，则持卡会员按下开始键 12b。认证单元 14 接受开始键 12b 的按下检测，而将有效期限以 4 位数(MM(月)/YY(年))显示出来。持卡会员根据该显示，在卡片信息输入画面 100 的有效期限输入栏 100b 中，输入有效期限。

此外，当显示器的显示领域、可显示位数还有余裕时，当然亦可将卡号一次全部显示在显示器上，又，亦可将卡号和有效期限一次全部显示出来。反之，当显示器的可显示位数少于 8 位数时，认证单元 14 可配合可显示位数，将从卡片信息存储部 13 中读出的卡片信息予以预先分割，通过检测开始键 12b 或其它任意键的按下，而依次地显示出已分割的卡片信息。

如上所述，网络结账辅助装置 1 仅当所输入的输入信息和认证信息存储部 15 中所存储的认证信息一致时，才在显示器 11 上显示卡片信息，因此，若不知道认证信息，则第三者即使盗取网络结账辅助装置 1，也无从得知内部的卡片信息。因此，相较于有印出卡片信息的现有信用卡，安全性较高，不会有卡

片信息被滥用于网络商业交易的疑虑。

持卡会员输入完卡号及有效期限(此外，图 4 的卡片信息输入画面 100 中虽未显示，但亦可将订购的商品.服务名、金额、订购日、加盟店名、商品的发送地等信息，显示于同一画面上)，便点击卡片信息输入画面 100 内的发送钮 100c。通过点击发送钮 100c，对加盟店终端 3 侧发送已输入的卡片信息(S10)。

从会员终端 2 接收到订购的商品·服务名、金额、订购日、加盟店名、商品的发送地等相关的订购信息；和订购商品的结账所用的卡片的卡号和有效期限等卡片信息的加盟店终端 3，除了已接收到的卡片信息以外，还将对每一加盟店赋予的加盟店识别信息，发送到通过网络 9a 而连接的中介服务器 5，要求确认持卡会员是否是能接受使用网络结账辅助装置 1 的商业交易服务的会员(认证执行可否确认)(S20)。

中介服务器 5 确认已收到的加盟店识别信息是否和所保有的加盟店识别信息一致(加盟店认证)。若这些信息一致，则从有参加使用网络结账辅助装置 1 的商业交易服务的加盟店的加盟店终端 3 访问中介服务器 5。若不一致，则由于来自没有参加使用网络结账辅助装置 1 的商业交易服务的加盟店的加盟店终端 3 的访问是不正当访问，因此不会进入之后的流程。

中介服务器 5 根据从有参加使用网络结账辅助装置 1 的商业交易服务的加盟店终端 3 所收到的持卡会员的卡片信息，确定出发行了该持卡会员的卡号的发卡银行，向已被确定的发卡银行的认证服务器 7，发送卡片信息，并要求确认持卡会员是否是能接受使用网络结账辅助装置 1 的商业交易服务的会员(认证执行可否确认)(S30)。

本实施例的中介服务器 5 中，存储有识别发卡银行的发卡银行识别信息，中介服务器 5 根据已收到的卡片信息来检索发卡银行识别信息，确定出发卡银行。

换言之，本实施例的中介服务器 5 并非直接进行认证执行可否确认，而是进行加盟店认证，并根据从加盟店终端 3 接收到的卡片信息，确定出发行了持卡会员的卡号的发卡银行，向已被确定的发卡银行的认证服务器 7 传送卡片信息，并负责将从该认证服务器 7 所接收到的认证执行可否确认结果传送至加盟

店终端 3。

此外，在本实施例中，中介服务器 5 虽然是由信用卡组织所营运的服务器，但亦可由各个加盟店终端 3 来具备，此时，就可直接从加盟店终端 3 向认证服务器 7，进行认证执行可否确认的要求。又，亦可在认证服务器 7 上，进行加盟店认证。

认证服务器 7 通过确认从中介服务器 5 所收到的卡片信息是否已被注册在认证服务器 7 中，来进行持有该卡片信息的持卡会员是否为能接受使用网络结账辅助装置 1 的商业交易服务的持卡会员的确认(认证执行可否确认)，并将其结果回送给中介服务器 5(S40)。此外，认证执行可否确认结果，若是从中介服务器 5 接收到的卡片信息已被注册在认证服务器 7 中则为「可」，若没有被注册则为「否」。

然后，接收到认证执行可否确认结果的中介服务器 5 将该结果传送至加盟店终端 3(S50)。

当持卡会员的认证执行可否确认结果为「可」时，则意味着该持卡会员是能接受使用网络结账辅助装置 1 的商业交易服务的，因此加盟店终端 3 进入进行该持卡会员的本人认证要求的流程(S60)。具体而言，加盟店终端 3 对会员终端 2 发送认证执行可否结果，并且还发送之前进行过认证执行可否确认的发卡银行的认证服务器 7 的 URL 信息。

从加盟店终端 3 收到认证要求的会员终端 2 根据所收到的 URL，向之前中介服务器 5 访问的同一认证服务器 7 进行访问，进行认证要求(S70)。此外，S70 的流程，是从 S60 起以一连串方式进行；可以使用作为会员终端 2 使用的个人计算机或手机的浏览器所一般具备的重新导向功能等来加以实现，让持卡会员不会有所意识，就可在会员终端 2 内部自动进行处理的流程。

认证服务器 7 向会员终端 2 催促一次性密码的发送，并根据从会员终端 2 所接收到的一次性密码，进行持卡会员的认证(S80)。

具体而言，认证服务器 7 从来访问的会员终端 2 接收卡片信息及订购信息，并确认拥有该卡片信息的持卡会员，是否为刚才从加盟店终端 3 通过中介服务器 5、受到认证执行可否确认要求的持卡会员。此确认是在预定的预定时间前留下是否从中介服务器 5 接收到该卡片会员的卡片信息的日志，并通过确认

从会员终端 2 接收到的持卡会员的卡片信息，是否和预定时间前留在日志中的卡片信息一致而进行的。

此外，订购信息也可不从会员终端 2 发送，而是在 S20、30 的流程中，从加盟店终端 3 通过中介服务器 5 而发送至认证服务器 7 的；或亦可在从加盟店终端 3 向会员终端 2 发送认证服务器 7 的 URL 信息时，一起被发送，而在会员终端 2 访问认证服务器 7 时，转送给认证服务器 7。

又，认证服务器 7 所进行的，对来访问的会员终端 2 的持卡会员、和从加盟店终端 3 接受了认证执行可否确认要求的持卡会员是否为同一个人的确认，可并不仅通过卡片信息的核对，而且还可从会员终端 2 及加盟店终端 3(直接通过中介服务器 5)双方接收订购信息，而一并进行这些信息的核对。

认证服务器 7，一旦确认了是来自之前接受了认证执行可否确认要求的持卡会员的网络结账辅助装置 1 的访问，则认证服务器 7 根据所收到的订购信息，生成如图 4(b)所示的一次性密码输入画面 101，并发送至进行了访问的会员终端 2。

图 4(b)的一次性密码输入画面 101 中，显示持卡会员正在进行网络商业交易的对象也就是加盟店名、欲订购的商品・服务的金额、订购日。

一旦在会员终端 2 上显示出一次性密码输入画面 101，则持卡会员按下网络结账辅助装置 1 的开始键 12b。网络结账辅助装置 1 的 OTP 生成单元 16 一旦检测到开始键 12b 按下，则从一次性密码生成等待状态，转移到一次性密码生成流程。

OTP 生成单元 16 将存储在 OTP 生成信息存储部 17 中的公共钥匙读出，通过计时单元 18 进行计时，将根据开始键 12b 被按下的日期时间所构成的日期时间数据(年月日秒、秒是以 30 秒为单位)，以该公共钥匙进行加密而生成一次性密码，并将其转换成 10 进制数，显示于显示器 11 上。此外，本实施例的加密方式是采用公共钥匙加密方式。又，由于本实施例的显示器 11 的可显示位数为 8 位数，因此显示器 11 上会显示出所生成的一次性密码的前 6～8 位数。

持卡会员在显示于会员终端 2 的一次性密码输入画面 101 的密码输入栏 101a 中，输入被显示在网络结账辅助装置 1 的显示器 11 上的一次性密码，并

点击发送钮 101b，则已输入的一次性密码会被发送至认证服务器 7。

此外，一次性密码的输入结束后，持卡会员再度按下网络结账辅助装置 1 的开始键 12b，就可使网络结账辅助装置 1 的显示器 11 上所显示的一次性密码变成不显示，这从安全性的观点来看较为理想。又在此同时，也将电源关闭，从节能观点来看较为理想。

从会员终端 2 接收到一次性密码的认证服务器 7，首先是通过会员终端 2 的识别号码等的核对、或该会员终端 2 个别生成并发送过来的对一次性密码输入画面 101 是否有回送的确认，来确认该会员终端 2 是否为刚才要求发送一次性密码的对方。

确认后，认证服务器 7 根据要求一次性密码的发送之前就接收到的持卡会员的卡片信息，从 OTP 生成信息中，取出和该卡号相关联而注册的公共钥匙，并将认证服务器 7 从会员终端 2 接收到一次性密码的日期时间所构成的日期时间数据(年月日秒、秒是以 30 秒为单位)，以该公共钥匙进行加密而生成一次性密码，并将其转换成十进制数。此外，本实施例的加密方式，是采用公共钥匙加密方式。

如此一来，认证服务器 7 确认认证服务器 7 所生成的一次性密码、和之前从会员终端 2 所接收到的一次性密码是否一致。若为一致，则可证明该一次性密码确实为通过仅存储于网络结账辅助装置 1 和认证服务器 7 的公共钥匙在几乎相同时刻所生成的一次性密码。

换言之，将一次性密码发送至认证服务器 7 的会员终端 2 的操作者，是存储有该一次性密码生成时所用的公共钥匙、及该公共钥匙所关联的卡片信息的网络结账辅助装置 1 的操作者；且是可利用该卡片信息的持卡会员本人，藉此，要求网络商业交易的持卡会员的本人确认就被进行了。

此外，一次性密码生成方式，是采用本实施例这种时间同步方式时，网络结账辅助装置 1 在生成一次性密码时所用的日期时间，和认证服务器 7 在生成一次性密码时所用的日期时间不一定严格地相同，因此，考虑到从认证服务器 7 生成一次性密码起，至持卡会员按下网络结账辅助装置 1 的开始键 12b，网络结账辅助装置 1 生成一次性密码为止的时间差，本实施例中，是将日期时间数据的秒分辨能力设为 30 秒。

可是，只有当由两者所生成的一次性密码是完全一致的情况下，才能认可持卡会员的真实性，持卡会员按下网络结账辅助装置 1 的开始键 12b 以生成一次性密码，若一直到认证服务器 7 从会员终端 2 接收一次性密码为止的期间是经过了 30 秒以上的情形下，只是这样使得一次性密码不一致导致无法认证的情况增加，反而会有损网络商业交易的便利性。

因此，认证服务器 7 当即使从会员终端 2 收到的一次性密码不一致时，仍会将从会员终端 2 收到的一次性密码的日期时间，往前后错开 N 次×30 秒的量，在认证服务器 7 侧重新生成一次性密码，若和会员终端 2 侧所生成的一次性密码一致，则视为持卡会员的本人确认成功。

此外，N 是考虑安全性的精度，而预先决定的。即，当想要提高安全性精度时，则将 N 设定得较小；当想要降低安全性精度而以持卡会员侧的便利性优先时，则将 N 设定得较大。

认证服务器 7 将一次性密码核对的持卡会员的认证结果，发送至会员终端 2(S90)。此外，具体而言，认证服务器 7 对会员终端 2，除了发送认证结果，还发送加盟店终端 3 的 URL 信息，并从会员终端 2 向加盟店终端 3 转送认证结果。

收到认证结果的会员终端 2 将该认证结果(本人认证 OK、本人认证 NG)，再转送至加盟店终端 3(S100)。此外，S100 的流程是和 S70 同样地，从 S90 起以一连串方式进行；可通过会员终端 2 的浏览器的重新导向功能来实现，实际上，是让持卡会员不会有所意识，而在会员终端 2 内部自动进行处理的流程。

加盟店终端 3 从会员终端 2 接收认证结果，且认证结果为，持卡会员被确认为本人时(本人认证 OK)，则向收单银行进行该持卡会员的授权要求，因此，向收单银行终端 4 除了发送持卡会员的卡片信息、和结账希望金额(持卡会员所欲订购的商品・服务的金额)所构成的交易数据以外，还发送该认证结果(S110)。此外，交易数据也可在 S10 中，从会员终端 2 有订购信息和卡片信息发送的时刻就已被生成，且被存储在加盟店终端 3 中，将其加以读出。

收单银行终端 4 根据从加盟店终端 3 接收到的交易数据和认证结果，并根据本人认证 OK 的持卡会员的卡号，来确定出卡片发行源的发卡银行，并向已

确定的发卡银行的发卡银行终端 6，转送交易数据和认证结果(S120)。

收到交易数据和认证结果的发卡银行终端 6 根据未图标的会员数据库中所存储的每位会员的会员信息或授信信息，来确认交易数据中所含的结账希望金额，是否为受到授权委托的持卡会员的信用额度范围内。若结账希望金额是在信用额度范围内，则作为授权 OK，确保结账希望金额量的信用额度。

然后，发卡银行终端 6 将授权的结果(授权 OK、授权 NG)发送至收单银行终端 4(S130)，然后收单银行终端 4 向加盟店终端 3 转送授权结果(S140)。

然后，加盟店终端 3 从收单银行终端 4 接收到授权结果后，将该结果通知给会员终端 2(S150)。具体而言，当授权结果为 OK 时，则加盟店和持卡会员之间，将使用该持卡会员的卡号的结账的网络商业交易成立的意思的画面发送至会员终端 2，并显示在会员终端 2 上。又，当授权结果为 NG 时，将网络商业交易不成立的意思的画面发送至会员终端 2，并显示。

此外，本实施例中，认证服务器 7 中的使用一次性密码的本人认证，是在会员终端 2 和加盟店终端 3 之间每次进行网络商业交易时就会进行的。换言之，本实施例的 OTP 生成单元 16 所生成的一次性密码，是仅限 1 次的网络商业交易中有效的，所以即使未持有网络结账辅助装置的第三者窃听到一次性密码，第三者仍无法伪装成持卡会员而进行之后的网络商业交易，因此可进一步提升商业交易的安全性。

实施例 2

其次，针对被发放网络结账辅助装置 1a(未图标)的持卡会员，使用该网络结账辅助装置 1a，由具有通信功能的个人计算机或手机，通过使用该持卡会员的卡号的结账，进行网络商业交易时的一实施例，加以说明。

本实施例和之前的实施例 1 的不同点在于，网络结账辅助装置所具备的 OTP 生成单元 16 的一次性密码生成方法、OTP 生成信息存储部 17 的存储内容、和图 3 中的会员终端 2 与认证服务器 7(本实施例中为认证服务器 7a)之间的认证流程(S80、S90)的内容。

即，在先前的实施例 1 中，一次性密码生成方法设为时间同步方式，但在本实施例中，是采用利用次数同步方式。伴随于此，本实施例的网络结账辅助

装置 1a 中，图 1 中所记载的计时单元 18 被取代成计数单元 18a(未图示)。

关于网络结账辅助装置 1、1a 和认证服务器 7、7a，由于除了上述不同点以外的构成，及 S80、S90 以外的流程是和图 1～图 3 所示的实施例相同的，所以以下使用图 1～图 3，仅说明图 3 的 S80、S90 的部分的详细流程。

本实施例的 OTP 生成信息存储部 17 中所存储的 OTP 生成信息，是由网络结账辅助装置 1a 所固有的公共钥匙，和利用次数信息所构成的。

其中，公共钥匙是以在 OTP 生成信息存储部 17 内不可改写的状态而被存储的，且在进行 OTP 生成单元 16 所生成的一次性密码的验证的认证服务器 7a 中，与被存储在卡片信息存储部 13 的卡号相关联。

利用次数信息和公共钥匙同样地，在认证服务器 7a 中，与卡片信息存储部 13 中所存储的卡号相关联。

换言之，这些 OTP 生成信息，是以和卡号相关联的状态，也在认证服务器 7a 中被存储的；当认证服务器 7a 从会员终端 2 接收到一次性密码时，与会员终端 2 同样地，认证服务器 7a 中也会生成一次性密码，通过确认两者是否一致，就可进行一次性密码的妥当性验证、持卡会员的认证。

又，利用次数信息，是仅当有来自 OTP 生成单元 16 的改写指令时才可改写的信息，通过计数单元 18a，0 次、1 次、2 次这种一次加 1 的加法，或 100 次、99 次、98 次这种一次减 1 的减法后，加法或减法后的数值，会被存储在 OTP 生成信息存储部 17 中，利用次数信息会被更新。此外，预先决定是加法还是减法。

此外，计数单元 18a，也可被包含在 OTP 生成单元 16，也可与 OTP 生成单元 16 分开设置，但后者的情况中，需要由 OTP 生成单元 16 来控制计数单元 18a，进行利用次数信息的改写。

图 3 的 S80 中，首先，认证服务器 7a 向会员终端 2 催促一次性密码的发送，并根据从会员终端 2 所接收到的一次性密码，进行持卡会员的认证。

具体而言，认证服务器 7a 从来访问的会员终端 2，接收卡片信息及订购信息，并确认拥有该卡片信息的持卡会员，是否为刚才从加盟店终端 3 通过中介服务器 5、受到认证执行可否确认要求的持卡会员。此确认是在预定的预定时间前留下是否从中介服务器 5 接收到该卡片会员的卡片信息的日志，并通过确

认从会员终端 2 接收到的持卡会员的卡片信息，是否和预定时间前留在日志中的卡片信息一致而进行的。

此外，订购信息，可不从会员终端 2 发送，而是在 S20、30 的流程中，从加盟店终端 3 通过中介服务器 5 而发送至认证服务器 7a；或亦可在从加盟店终端 3 向会员终端 2 发送认证服务器 7a 的 URL 信息时，一起被发送，而在会员终端 2 访问认证服务器 7a 时，转送给认证服务器 7a。

又，认证服务器 7a 所进行的，来访问的会员终端 2 的持卡会员、和从加盟店终端 3 接受了认证执行可否确认要求的持卡会员是否为同一个人的确认，可不仅通过卡片信息的核对，而且可从会员终端 2 及加盟店终端 3(直接通过中介服务器 5)双方接收订购信息，而一并进行这些信息的核对。

认证服务器 7a 一旦确认了是来自之前接受了认证执行可否确认要求的持卡会员的网络结账辅助装置 1 的访问，则认证服务器 7a 根据所收到的订购信息，生成如图 4(b)所示的一次性密码输入画面 101，并发送至进行了访问的会员终端 2。

图 4(b)的一次性密码输入画面 101 中，显示持卡会员正在进行网络商业交易的对象也就是加盟店名、欲订购的商品・服务的金额、订购日。

一旦在会员终端 2 上显示出一次性密码输入画面 101，则持卡会员按下网络结账辅助装置 1 的开始键 12b。网络结账辅助装置 1 的 OTP 生成单元 16 一旦检测到开始键 12b 按下，则从一次性密码生成等待状态转移到一次性密码生成流程。

OTP 生成单元 16 将 OTP 生成信息存储部 17 中所存储的公共钥匙和利用次数信息予以读出，并将该利用次数信息，以公共钥匙加密而生成一次性密码，将其转换成 10 进制数，显示于显示器 11 上。

此外，本实施例中，是将利用次数信息使用预定的一次性密码生成算法，来生成一次性密码。

又，由于本实施例的显示器 11 的可显示位数是为 8 位数，因此显示器 11 上会显示出所生成的一次性密码的前 6～8 位数。

此外，OTP 生成信息除了上述利用次数信息和公共钥匙以外，亦可含有其它仅网络结账辅助装置 1a 与认证服务器 7a 两者可获知的任意信息(例如，原则

(policy)等)；此时，也可将利用次数信息、和该任意的信息用公共钥匙加密，来生成一次性密码。

OTP 生成单元 16 在生成一次性密码后，对计数单元 18a，将刚才读出的利用次数信息，加上或减去 1，然后将 OTP 生成信息存储部 17 的利用次数信息予以改写、更新。

持卡会员在显示于会员终端 2 的一次性密码输入画面 101 的密码输入栏 101a 中，输入被显示在网络结账辅助装置 1 的显示器 11 上的一次性密码，并点击发送钮 101b，则已输入的一次性密码会被发送至认证服务器 7a。

此外，一次性密码的输入结束后，持卡会员再度按下网络结账辅助装置 1 的开始键 12b，就可使网络结账辅助装置 1 的显示器 11 上所显示的一次性密码变成不显示，这从安全性的观点来看较为理想。又在此同时，也将电源关闭，从省电观点来看较为理想。

从会员终端 2 接收到一次性密码的认证服务器 7a，首先是通过会员终端 2 的识别号码等的核对、或该会员终端 2 个别生成并发送过来的对一次性密码输入画面 101 是否有回送的确认，来确认该会员终端 2 是否为刚才要求发送一次性密码的对方。

确认后，认证服务器 7a 根据要求一次性密码的发送之前就接收到的持卡会员的卡片信息，从 OTP 生成信息中，取出和该卡号相关联注册的公共钥匙和利用次数信息，并将利用次数信息以公共钥匙加密而生成一次性密码，并将其转换成十进制数。

此外，本实施例中，是将利用次数信息使用预定的一次性密码生成算法，来生成一次性密码。又，OTP 生成信息中，若含有任意的信息，则除了利用次数信息以外，该任意信息也会一并用公共钥匙加密。

如此一来，认证服务器 7a 确认认证服务器 7a 所生成的一次性密码、和之前从会员终端 2 所接收到的一次性密码是否一致。若为一致，则可证明该一次性密码确实为通过仅存储于网络结账辅助装置 1 和认证服务器 7a 的利用次数信息和公共钥匙所生成的一次性密码。

换言之，将一次性密码发送至认证服务器 7a 的会员终端 2 的操作者，是储存有该一次性密码生成时所用的利用次数信息和公共钥匙、及该利用次数信

息和公共钥匙相关联的卡片信息的网络结账辅助装置 1 的操作者；且是可利用该卡片信息的持卡会员本人，藉此，要求网络商业交易的持卡会员的本人确认就被进行了。

认证服务器 7a 将一次性密码核对所致的持卡会员的认证结果(本人认证 OK、本人认证 NG)发送至会员终端 2，并且还将之前一次性密码生成时所用到的利用次数信息，以预先决定的运算方法进行加法或减法，并将其运算结果当成认证服务器 7a 内的利用次数信息，加以改写、更新。

此外，一次性密码生成方式，在采用如本实施例的利用次数同步方式时，即使会员终端 2 及网络结账辅助装置 1a 的操作者是正当的持卡会员，可是仍有可能因网络结账辅助装置 1a 在生成一次性密码时所用的利用次数信息、和认证服务器 7a 在生成一次性密码时所用的利用次数信息不同，导致一次性密码不一致的情形。

持卡会员，即使以网络结账辅助装置 1a 生成一次性密码，但也并不能保证必定会被发送至认证服务器 7a，当持卡会员在网络商业交易的中途不慎发生断线时，或者，有可能原本就不是要进行网络商业交易，而是操作网络结账辅助装置 1a 来玩弄而不慎生成了一次性密码。此种情况下，由于网络结账辅助装置 1a 的利用次数信息是被更新，可认证服务器 7a 的利用次数信息未被更新，所以，当然所生成的一次性密码就不会一致。

可是，若只有当被两者所生成的一次性密码是完全一致的情况下，才能认可持卡会员的真正性，则会导致认证 NG 增加，反而有损网络商业交易的便利性。

因此，认证服务器 7a 当即使从会员终端 2 收到的一次性密码是不一致时，仍会将认证服务器 7a 中所存储的利用次数信息在预定范围(例如，利用次数信息+N)内加以变更，在认证服务器 7a 侧重新生成一次性密码，若和会员终端 2 侧所生成的一次性密码一致，则视为持卡会员的本人确认成功。

此外，N 是考虑安全性的精度，而预先决定的。即，当想要提高安全性精度时，则将 N 设定得较小；当想要降低安全性精度而以持卡会员侧的便利性优先时，则将 N 设定得较大。

如上所述，若使用本发明的网络结账辅助装置来进行网络商业交易，则在

将卡片信息输入至卡片信息输入画面时，被输入至网络结账辅助装置的输入信息，只要和网络结账辅助装置中所存储的认证信息不一致，则即使是持卡会员自身也无从得知卡片信息，因此，和卡片信息会泄漏的现有的信用卡不同，卡片信息的隐匿性较高，可防止网络商业交易中的卡片信息的不正当使用。

又，由于网络结账辅助装置为可移动型，因此无论持卡会员身处何处，都可使用手机、家中的个人计算机、外出地的个人计算机，来进行安全的网络商业交易，增加网络商业交易的便利性。

又，网络商业交易被进行时的持卡会员的本人认证，是依据网络结账辅助装置所生成的一次性密码、和认证服务器所生成的一次性密码是否一致而进行的。

此一次性密码，是网络结账辅助装置所固有的，且仅被存储在网络结账辅助装置及认证服务器中，而且是使用即使是持卡会员自身都无从得知的公共钥匙，将在每次检测到预定键按下的日期时间所构成的日期时间数据或者一次性密码的生成时就被更新的利用次数信息予以加密而形成的。

即，由于是只有正在操作网络结账辅助装置的持卡会员才能生成的认证信息，因此不持有网络结账辅助装置的第三者，是无法假冒持卡会员来进行网络商业交易的，可进一步提升网络商业交易的安全性。

而且，该一次性密码的生成，是只有在网络结账辅助装置上显示了卡片信息后才会进行的，因此，不具有网络结账辅助装置的第三者，即使只是知道卡号，也不能生成一次性密码。又，即使第三者窃得了网络结账辅助装置，若没有输入至网络结账辅助装置的认证信息，也无法生成一次性密码。换言之，由于无论第三者是否有得到网络结账辅助装置，都无法假冒持卡会员来进行网络商业交易，因此商业交易的安全性可受到保证。

此外，一次性密码的生成方法不限于上述实施例的时间同步方式，只要是在网络结账辅助装置和认证服务器之间，能够进行拥有网络结账辅助装置的持卡会员的本人认证即可。

又，由于网络结账辅助装置采用网络非连接型的构成，所以一度被存储于网络结账辅助装置中的卡片信息、认证信息、OTP 生成信息，是由于不正当访问等无法读出的，而且就连被发放网络结账辅助装置的持卡会员，也无法将其

读出。

假设，若网络结账辅助装置是可连接个人计算机或手机等终端的，则当网络结账辅助装置和终端的连接中，发生了某种不良情况时，该不良的原因，究竟是在网络结账辅助装置侧、还是在终端侧，此种责任划分点不明确。因此，采用网络非连接型的构成的网络结账辅助装置，对于责任划分点的明确而言，是有效的。

此处，将不持有网络结账辅助装置的持卡会员，在本实施例的网络结账系统中，进行网络商业交易时的事先注册的系统构成及流程，示于图 6。

持卡会员从会员 PC，向卡片公司(信用卡组织或发卡银行)所营运的持卡会员专用的 WEB 网站进行访问，并输入只有持卡会员知道的会员信息(出生年月日、电话号码、账户号码等)，发送至 WEB 网站(图 6 中，(1))。

接收到会员信息的卡片公司的 WEB 网站，向注册有该会员信息的卡片公司的基干系统进行访问，并向基干系统委托进行所收到的会员信息、和基干系统中所注册的会员信息的核对(图 6 中，(2))。基干系统向 WEB 网站回送核对结果(图 6 中，(3))。

若核对结果为 OK，则视为持卡会员的本人确认成功，并从 WEB 网站向会员 PC 要求密码的注册。会员 PC 将密码发送给 WEB 网站(图 6 中，(4))。

从会员 PC 接收到密码的 WEB 网站将该密码注册至卡片公司的认证服务器 7(图 6 中，(5))。

此处所注册的密码为固定密码，并非在网络结账辅助装置上所生成的那种一次性密码。换言之，未持有网络结账辅助装置的持卡会员，在网络结账系统上进行网络结账时，持卡会员的认证方法是只能通过固定密码的方法；一旦卡号和固定密码被第三者一度获知，则以后第三者就能够假冒持卡会员来进行网络结账。

又，未持有网络结账辅助装置的持卡会员为了注册密码，而向持卡会员的 WEB 网站进行访问，经过本人认证后才能进行密码注册作业，因此对持卡会员侧造成的负担较大。

进一步地，不只是持卡会员的负担大，即使在卡片公司侧，也需要构建用来让持卡会员注册密码的 WEB 网站，构建用来进行持卡会员的本人认证的基

干系统。

又，网络结账辅助装置的结构为：通常不会泄漏卡号，而仅为持卡会员所获知，或只有在输入了仅持卡会员具有的认证信息，才会显示出卡号；进一步地，由于网络结账时，持卡会员的本人认证所使用的密码并非固定密码，而是一次性密码，因此，第三者要假冒持卡会员来进行网络商业交易是极为困难的。

以上，虽然说明了网络结账辅助装置 1 的实施例，但是，本发明的网络结账辅助装置并非被限定于具备上述实施例所说明的全部构成要件的网络结账辅助装置 1，而可作各种变更及修正，实现每个目的所必须的构成要件可任意组合，来构成本发明的网络结账辅助装置。又，关于所述变更及修正也当然属于本发明的权利要求范围中。

例如，在实施例中，虽然说明了使用信用卡的卡号的网络结账，但只要是至少通过卡号来进行网络结账的卡片，除了信用卡以外，像是转帐卡等卡片的实施例，也属于本发明的权利要求范围中。

又，本实施例中，虽然是在利用卡片结账的网络商业交易中所使用的，但当持卡会员只希望进行网络商业交易，不希望现有的塑料型磁卡、IC 卡等所构成的信用卡所致的真实的面对面交易的情况下，亦可不接受信用卡的发行；本发明的网络结账辅助装置的拥有者不一定需要持有现有的塑料型的信用卡。

又，例如，实施例中虽然说明了，1 个网络结账辅助装置 1 的卡片信息存储部 13 中，存储有具有 1 种卡片信息的 1 持卡会员的卡片信息，并在认证信息存储部 15 中存储 1 种认证信息的情形，但亦可在卡片信息存储部 13 中存储多个卡号。此时的认证信息，既可是为了显示多个卡号而公用的认证信息，也可是卡号和认证信息分别对应，根据所输入的认证信息不同，显示器 11 上显示的卡号也不同。

又，母子信用卡等、同一或多个卡号被多人使用的情况中，既可根据每个人而存储不同的认证信息在认证信息存储部 15 中，也可存储公用的认证信息。

又，上述实施例中，虽然叙述了卡片信息和 OTP 生成信息，是在网络结账辅助装置 1、1a 及认证服务器 7、7a 分别相关联的，但为了防止卡片信息的

窃听，而将卡片信息和 OTP 生成信息以非直接的、间接的方式相关联，也包含于权利要求范围中。

具体而言，图 3 的 S10 中被会员终端 2 输入的卡片信息在 S20、30 中，经由加盟店终端 3、中介服务器 5，最终被发送至认证服务器 7、7a，但是，认证服务器 7、7a 在此时，将所收到的卡片信息中的卡号转换成和该卡号不同的独特的号码，并经由中介服务器 5，发送至加盟店终端 3(S40、50 中)。

进一步地，该独特的号码从加盟店终端 3 被发送至会员终端 2，经由会员终端 2 而被发送至认证服务器 7、7a(S60、70 中)。

接收到该独特的号码的认证服务器 7、7a 通过和最初把卡号转换成独特的号码时相反的转换规则，将独特的号码转换成卡号，将转换成的卡号所关联到的 OTP 生成信息，用于一次性密码的生成。

如此，通过使卡号和卡号以外的独特的号码和 OTP 生成信息相关联，除了 S10、S20、S30 中卡号被发送以外，在网络 9a 上都不会有卡号流通，因此卡号被窃听的可能性会大幅降低，对安全性的提升有所贡献。

又，上述实施例中虽然说明了，会员终端 2 向加盟店终端 3 发送卡片信息，认证服务器 7、7a 根据来自加盟店终端 3 的委托，而于图 2 的 S80 中，进行持卡会员的本人认证的情形，但是，本发明并不一定局限于此。

例如，亦可先由会员终端 2 访问认证服务器 7，然后认证服务器 7、7a 会将持卡会员专用的认证信息输入画面发送给会员终端 2，根据被输入至该认证输入画面的卡片信息和一次性密码，在会员终端 2 和认证服务器 7、7a 之间进行持卡会员的本人认证；在其结果为确认是本人以后，在预定条件(例如预定时间、预定次数、预定加盟店等)内，由会员终端 2 访问加盟店终端 3 的网站，而进行网络商业交易。

换言之，本发明的网络结账辅助装置，基本上是设计成用于在会员终端 2、和卡片公司侧的认证服务器 7、7a 之间，进行持卡会员的本人认证，且在认证后，就可实际在加盟店的网站等中进行网络商业交易；不一定要以来自加盟店终端 2 的本人认证委托为前提。

本发明中的各单元、数据库仅在逻辑上区别其功能，在实体上或事实上也可成为同一领域的。又，当然也可取代数据库改用数据文件，和数据库的记载

中也包含数据文件。

上述实施例中，虽然说明了，网络结账系统上的终端或服务器，是信用卡组织(商业交易服务的提供主体)、发卡银行(持卡会员的获得·对持卡会员发行卡片的主体)、收单银行(加盟店的获得·契约·管理主体)、加盟店各自所营运的，但是，这些都仅是概念上、角色上的区别，实体上，会有发卡银行和收单银行为同一者的情形，或也有信用卡组织、发卡银行、收单银行为同一者的情形。

因此，例如，于本说明书中，网络结账辅助装置 1、1a 并非被限定于由发卡银行所发放。又，网络结账系统的提供主体也不一定必须是信用卡组织。又，发卡银行终端 6 和认证服务器 7、7a 和收单银行终端 4 也可为同一者。又，中介服务器 5、其它终端或服务器的任一个均可以是同一者。

此外，实施本发明时，是将存储有实现本实施方式的功能的软件的程序的存储介质提供给系统，由该系统的计算机将存储介质中所存储的程序加以读出并执行，而加以实现。

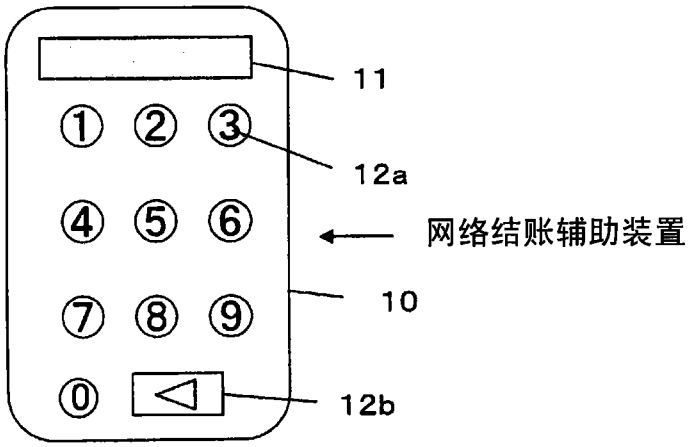
此时，从存储介质中读出的程序自身会实现实施方式的功能，存储有该程序的存储介质构成本发明。

作为用来提供程序的存储介质，例如可使用磁盘、硬盘、光盘、光磁盘、磁带、非易失性存储卡等。

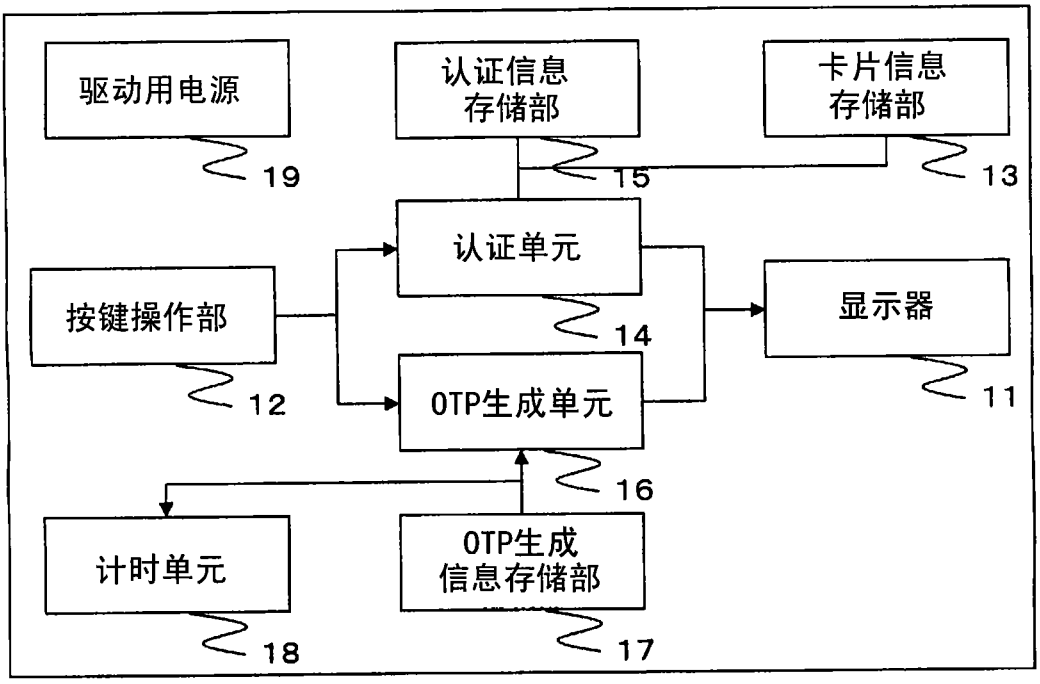
又，不仅是通过计算机执行已读出的程序来实现上述实施方式的功能，而且根据该程序的指示，由计算机上运作中的操作系统等进行实际处理的部分或全部，并通过该处理来实现所述实施方式的功能的情况，也被涵盖在本发明中。

进一步地，从存储介质中被读出的程序被写入至被插入在计算机中的功能扩充板或连接至计算机的功能扩充单元上所具备的非易失性或易失性的存储单元后，根据该程序的指示，由功能扩充板或功能扩充单元所具备的运算处理装置等来进行实际的处理的部分或全部，通过该处理来实现所述实施方式的功能的情况，也被涵盖在本发明中。

(a)



(b)



↑网络结账辅助装置1

图 1

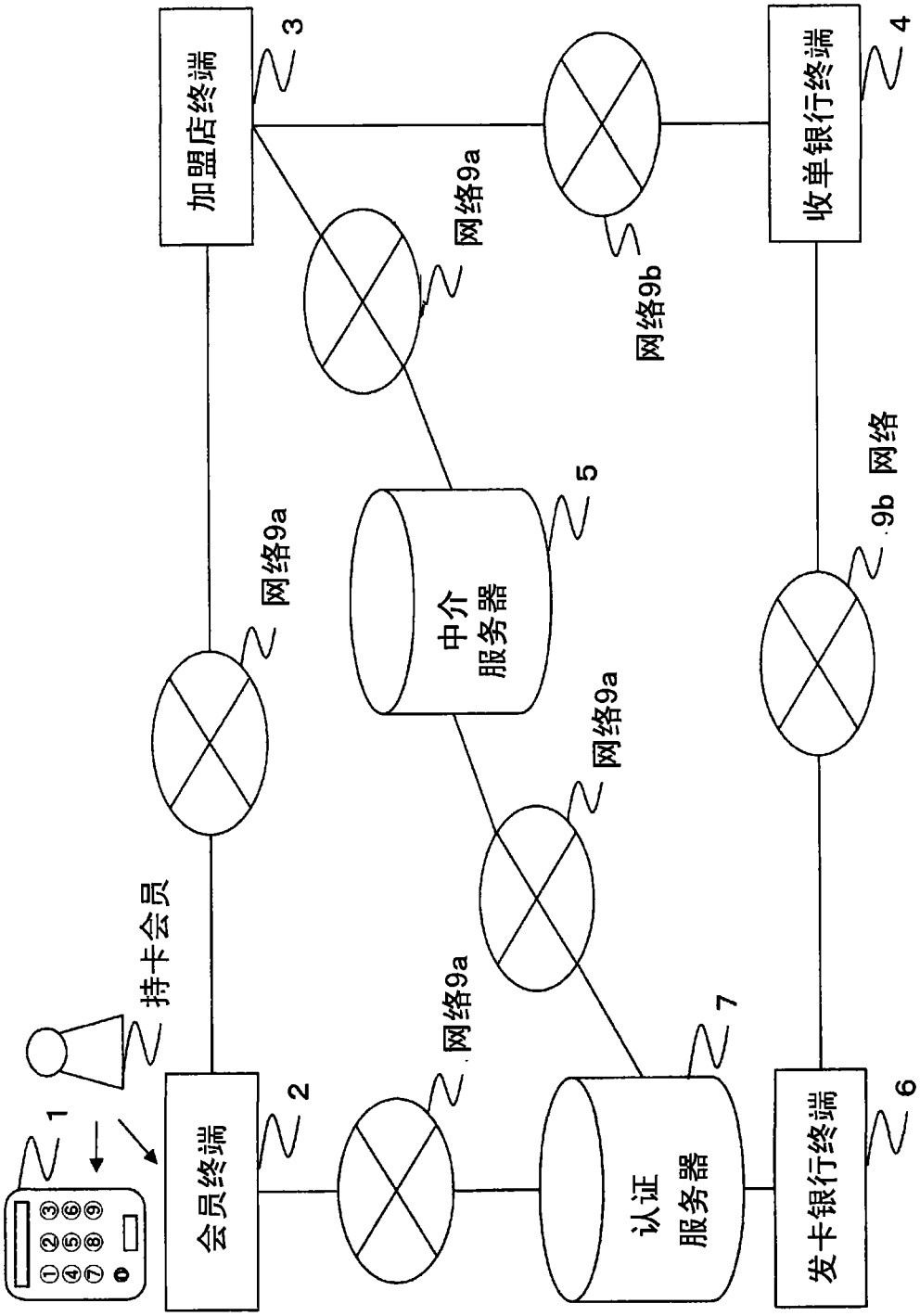

加盟店终端
3
收单银行终端
4
网络9a
网络9b
网络9a
中介
服务器
5
网络9a
网络9a
网络9b 网络
持卡会员
1
会员终端
2
网络9a
认证
服务器
7
发卡银行终端
6
网络结账系统

图 2

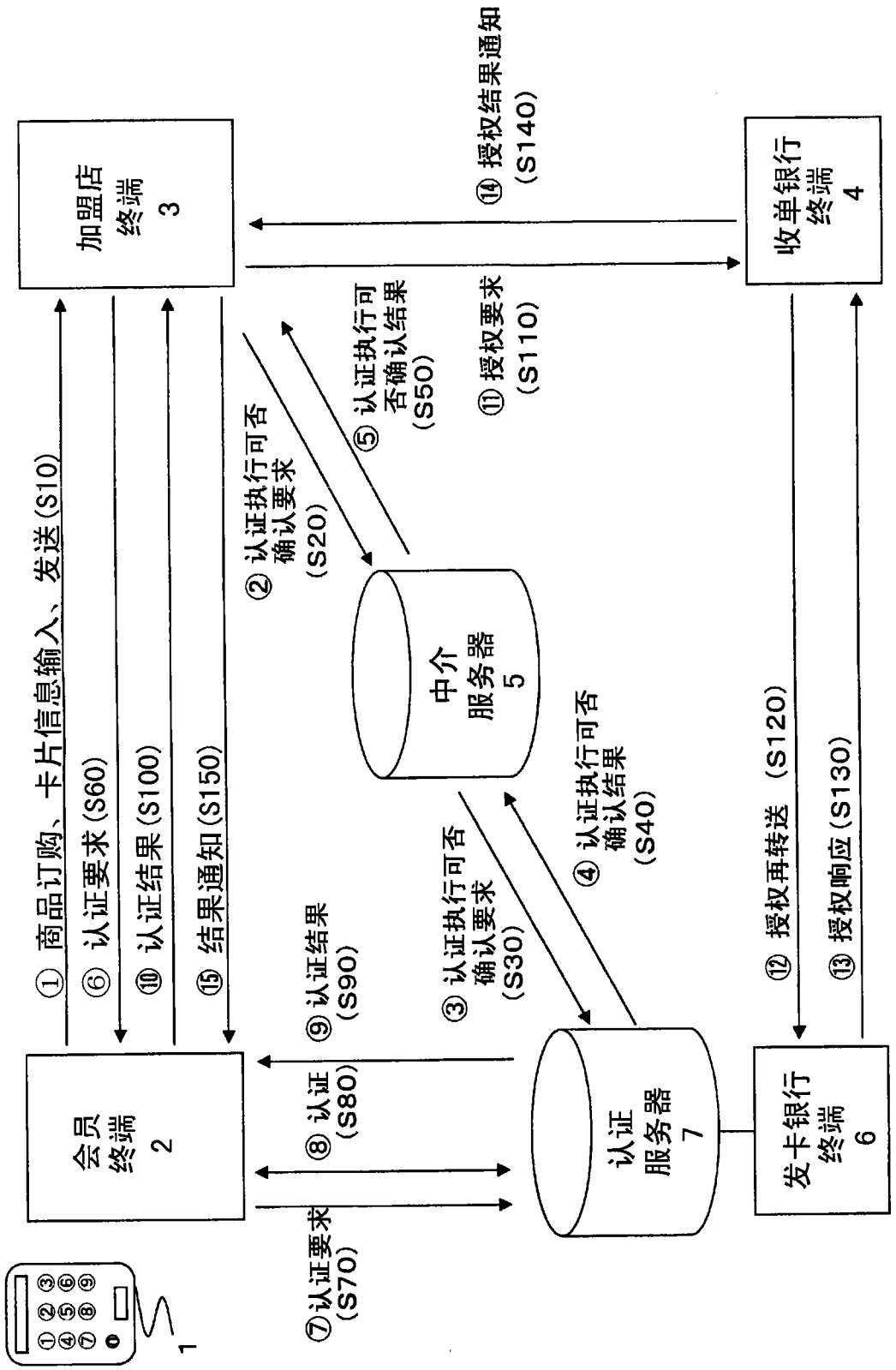

加盟店
终端
3
收单银行
终端
4
中介
服务器
5
会员
终端
2
认证
服务器
7
发卡银行
终端
6
1
① 商品订购、卡片信息输入、发送(S10)
② 认证执行可否
确认要求
(S20)
③ 认证执行可否
确认要求
(S30)
④ 认证执行可否
确认结果
(S40)
⑤ 认证执行可
否确认结果
(S50)
⑥ 认证要求(S60)
⑦认证要求
(S70)
⑧ 认证
(S80)
⑨ 认证结果
(S90)
⑩ 认证结果(S100)
⑪ 授权要求
(S110)
⑫ 授权再转送 (S120)
⑬ 授权响应(S130)
⑭ 授权结果通知
(S140)
⑮ 结果通知(S150)

图 3

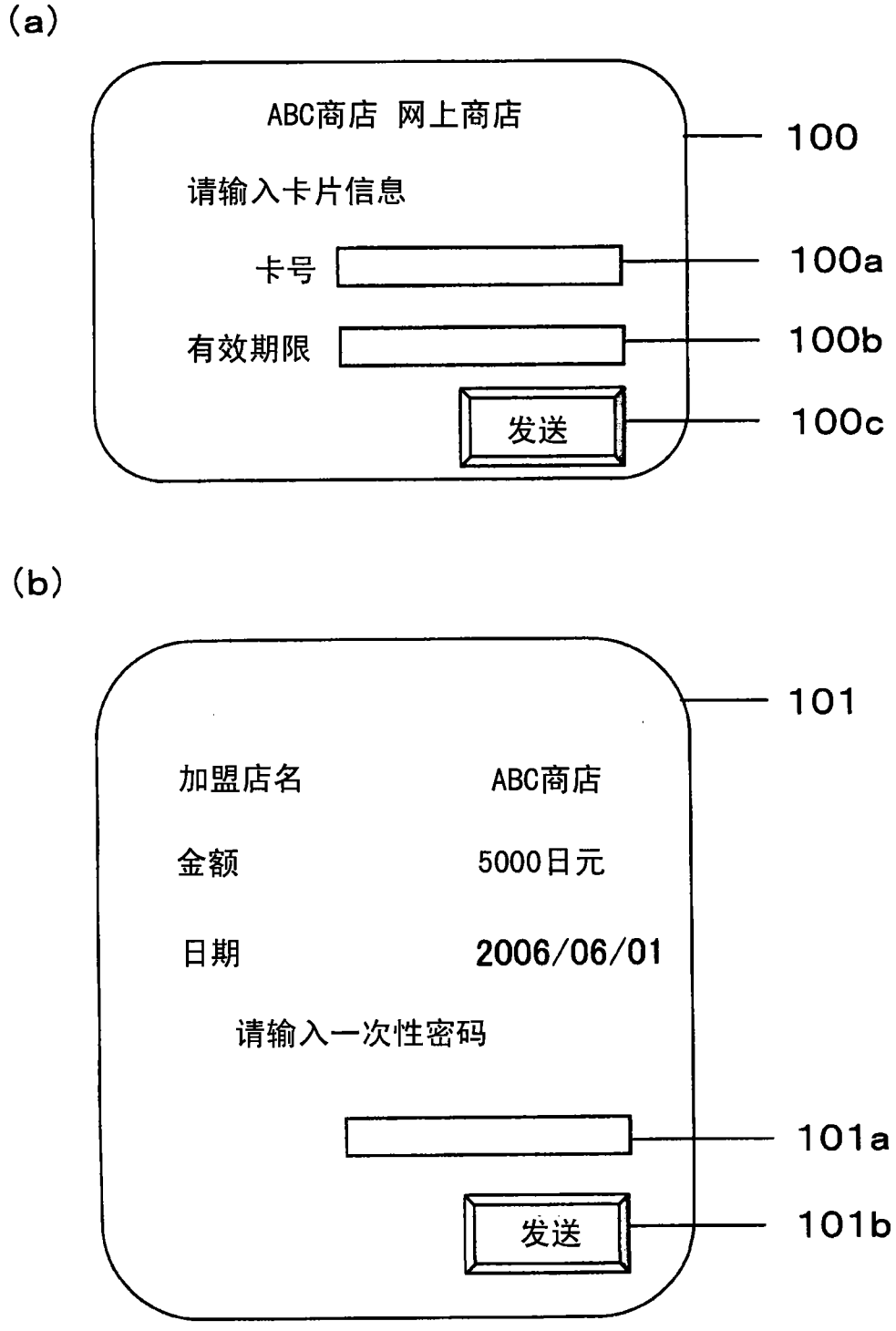

(a)
ABC商店 网上商店
请输入卡片信息
卡号
有效期限
发送
100
100a
100b
100c
(b)
加盟店名
ABC商店
金额
5000日元
日期
2006/06/01
请输入一次性密码
发送
101
101a
101b

图 4

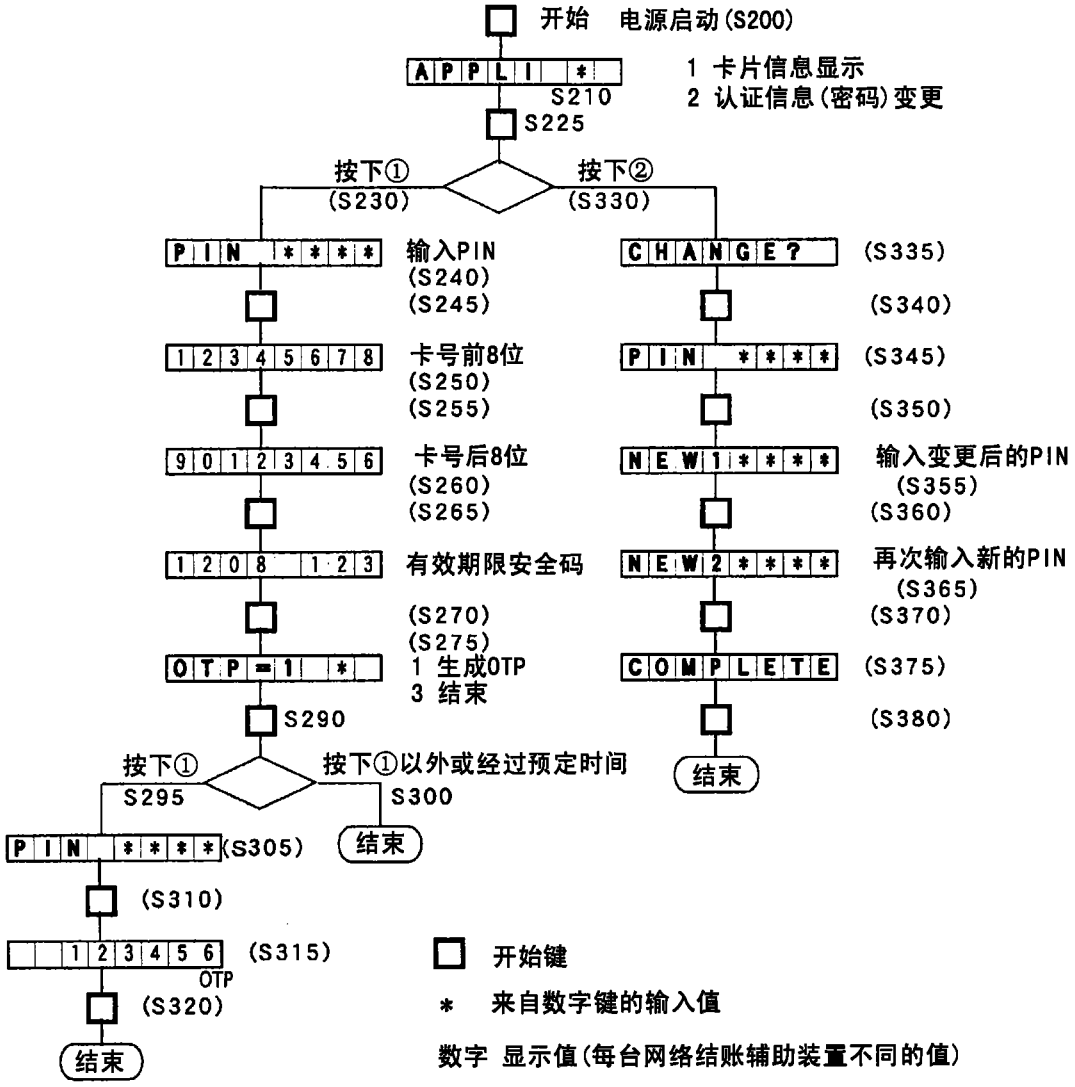

开始 电源启动(S200)
APPLI *
S210
1 卡片信息显示
2 认证信息(密码)变更
S225
按下①
(S230)
按下②
(S330)
PIN ****
输入PIN
(S240)
(S245)
12345678
卡号前8位
(S250)
(S255)
90123456
卡号后8位
(S260)
(S265)
1208 123
有效期限安全码
(S270)
(S275)
OTP=1 *
1 生成OTP
3 结束
S290
按下①
S295
按下①以外或经过预定时间
S300
结束
PIN ****(S305)
(S310)
123456
OTP
(S315)
(S320)
结束
CHANGE?
(S335)
(S340)
PIN ****
(S345)
(S350)
NEW1****
输入变更后的PIN
(S355)
(S360)
NEW2****
再次输入新的PIN
(S365)
(S370)
COMPLETE
(S375)
(S380)
结束
开始键
* 来自数字键的输入值
数字 显示值(每台网络结账辅助装置不同的值)
粗体字 引导(每台网络结账辅助装置共同规格)

图 5

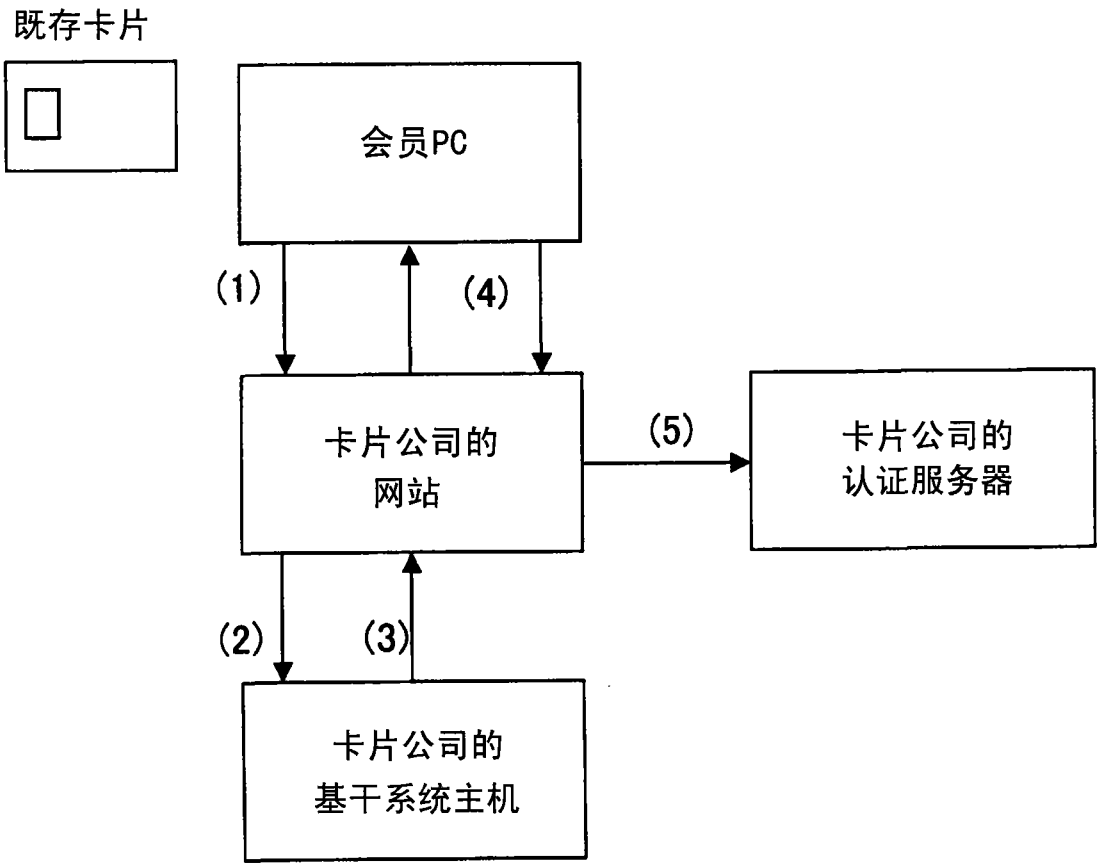


图 6