[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/20 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 200580040921.X

[45] 授权公告日 2009 年 4 月 29 日

[11] 授权公告号 CN 100483436C

[22] 申请日 2005.11.1
[21] 申请号 200580040921.X
[30] 优先权
[32] 2004.11.29 [33] JP [31] 344277/2004
[86] 国际申请 PCT/JP2005/020092 2005.11.1
[87] 国际公布 WO2006/057140 日 2006.6.1
[85] 进入国家阶段日期 2007.5.29
[73] 专利权人 王 祝
地址 日本东京
共同专利权人 东京电力株式会社
[72] 发明人 重富孝士 刈本博保 中村正规
[56] 参考文献
WO2004/077208A2 2004.9.10
CN1139894C 2004.2.25
US2002/0095588A1 2002.7.18
US2003/0074568A1 2003.4.17
JP11-7412A 1999.1.12
US2001/0044900A1 2001.11.22
JP2003-9243A 2003.1.10
US6148094A 2000.11.14
审查员 李 强
[74] 专利代理机构 北京君尚知识产权代理事务所
代理人 余功勋

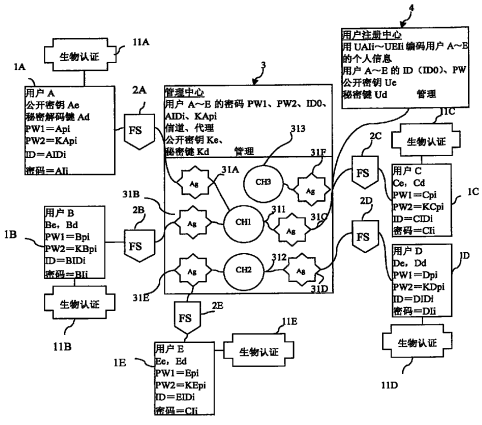
权利要求书 2 页 说明书 12 页 附图 5 页

[54] 发明名称

网络访问系统、方法以及存储介质

[57] 摘要

仅事先在网络中登记的用户才可以访问网络，该网络具有非常高的安全性。 用于对用户(1A)进行生物认证的生物认证信息和已确定的每个用户访问网络所必需的访问认证信息存储在安装于磁盘的电子电路的存储器(外部存储介质)中。 磁盘驱动时，通过生物认证装置(11E)，从用户获取生物认证信息，于存储在电子电路(外部存储介质)中的生物认证信息进行比较，当两个信息一致时，将存储在电子电路(外部存储介质)中的访问认证信息发送至网络中。 在网络中，根据接收到的访问认证信息，判断用户是否是正规用户，当判断是正规用户时，许可上述用户终端通过其调谐服务器经由上述网络服务社区中的相应代理商连接到上述网络服务社区中的特定网络服务信道。



1．一种网络访问方法，其用于通过经由网络的用户终端的访问进行与网络服务社区的连接，该社区含有在由管理中心管理的服务器中运行的特定网络服务信道，在上述管理中心服务器存储用户的个人信息和许可连接的用户的访问认证信息，上述用户终端具有或连接有检测用户生物认证信息的生物认证信息检测装置，以及连接有存储上述用户生物认证信息和决定每个用户访问网络时必要的访问认证信息、具有信号处理功能的外部存储介质，其步骤包括：

将由上述生物认证信息检测装置检测的来自用户的生物认证信息与存储在上述外部存储介质中的生物认证信息进行比较，当两个信息一致时，存储在上述外部存储介质中的上述访问认证信息经由上述用户终端发送给上述管理中心，

在接收到的上述访问认证信息与预先存储的访问认证信息一致的情况下，上述管理中心判断上述用户是注册的正规用户，并许可上述用户终端通过其调谐服务器经由上述网络服务社区中的相应代理商连接到上述网络服务社区中的特定网络服务信道。

2．根据权利要求 1 记载的网络访问方法，其特征在于：上述外部存储介质为磁盘，由连接在上述用户终端的磁盘驱动器驱动，该磁盘的电子电路存储上述用户生物认证信息和决定每个用户访问网络时必要的访问认证信息。

3．根据权利要求 1 记载的网络访问方法，其特征在于：上述管理中心具有内置的或与其连接的用户注册中心，在上述用户注册中心存储有上述访问认证信息。

4．根据权利要求 1 或 3 记载的网络访问方法，其特征在于：上述访问认证信息含有用户的 ID 和密码。

5．根据权利要求 1 或 3 记载的网络访问方法，其特征在于：上述用户在上述管理中心的信息发送接收通过对上述用户预先赋予的昵称进行。

6．根据权利要求 3 记载的网络访问方法，其特征在于：上述访问认证信息被编码后从上述用户终端侧输出，在上述管理中心和用户注册中心，对接收到的编码后的上述访问认证信息进行解码。

7．根据权利要求 6 记载的网络访问方法，其特征在于：上述用户和上述管理中心和用户注册中心之间的信息发送接收是通过使用公开密钥的编码和使用对应于上述公开密钥的秘密解码键的解码处理进行的。

8．根据权利要求 7 记载的网络访问方法，其特征在于：上述访问认证信息在上述用户每次访问时变化，仅上述用户终端和上述管理中心和用户注册中心得知上述变化。

9．根据权利要求 8 记载的网络访问方法，其特征在于：上述用户终端产生上述用户下次访问使用的访问认证信息并对该访问认证信息进行编码后发送到上述管理中心，由管理中心解码后保存，在下次从上述用户终端访问时，上述用户终端发送更新后的上述访问认证信息。

10．根据权利要求 3 记载的网络访问方法，其特征在于：存储在上述管理中心服务器中的与用户有关的个人信息由上述每个用户的基本码管理，确定上述用户的用户个人信息仅通过基本码才可以读取、写入，该基本码是由上述用户终端侧的外部存储介质产生的辅助码和该用户的基础码组合而产生，所述基础码为上述用户注册中心赋予该用户的唯一编码。

11．根据权利要求 10 记载的网络访问方法，其特征在于：上述基本码由上述用户终端采用管理中心的公开密钥编码后从上述用户终端发送管理中心，在上述管理中心，通过对应于上述公开密钥的秘密解码键解码后作为得到的基本码使用。

12．根据权利要求 1 或 3 记载的网络访问方法，其特征在于：上述用户生物认证信息是指纹认证、容貌认证、声音认证或眼睛的虹膜认证。

13．根据权利要求 2 记载的网络访问方法，其特征在于：上述磁盘是光盘。

网络访问系统、方法以及存储介质

技术领域

本发明涉及网络访问系统、方法以及存储介质，特别是涉及可以保持高度安全性的网络访问系统、方法以及存储介质。

背景技术

随着互联网以及宽带环境的迅速普及，个人通过于互联网可以享受各种服务。每个用户在自己家里使用个人电脑或便携终端可以容易地访问网络服务。

在这种服务中，如果仅在一方接收信息，仅下载该信息，就不用担心用户个人信息的泄漏，但是对于诸如网络竞卖、商品买卖等的电子商务，由于必须公开用户的个人信息，所以具有信息泄漏的危险。这种电子商务系统，例如公开在专利文献 1 中。

专利文献 1：特开 2004－318497（图 1，第[0009]～[0016]段）

发明内容

但是，在电子商务中，必须公开用户的信用卡卡号和有效期、个人银行帐户、住址、姓名、出生日期等个人信息的情况很多。此外，在网络上输入的个人信息，委托给对方使用处理，所以不能保证个人信息的安全性，尤其是特别担心该个人信息在网络中被无限地传播，随时会被传送给其他人。

因此，为了确保安全性，利用用于认证用户本人的各种认证方法（ID 和密码）的系统被加以实际应用。但是，这种认证系统总是存在漏洞，具有利用系统的弱点盗取个人信息或修改个人信息的情况。为了进一步提高认证系统的安全性，虽然为每次服务设定 ID 和密码是有效的，但是由于用于其管理的费用大多要由用户负担，因此在成本方面存在问题。

此外，利用该个人信息假冒用户进行电子商务的危险性很大。除了假冒用户，由于恶意商家加入可靠的 e 商务，即使在著名的站点也具有被假冒的危险。

进一步地，通过作为网络服务一环的邮件加入社区的服务时，由于在相关的服务中，用户的邮件地址被公开给第三方，所以还具有在不知情的情况下被垃圾邮件骚扰的担心。

本发明正是鉴于现有技术的上述问题提出的，主要目的在于提供可以克服这些问题的

网络访问系统、方法以及存储介质。

用于解决上述问题的本发明的网络访问系统、方法以及存储介质采用如下特征的结构。

1．一种网络访问方法，其用于通过经由网络的用户终端的访问进行与网络服务社区的连接，该社区含有在由管理中心管理的服务器中运行的特定网络服务社会信道（社会），其特征在于：

在上述管理中心服务器存储用户的个人信息和许可连接的用户的访问认证信息，

该网络访问系统包括：上述用户终端具有或连接有检测用户生物认证信息的生物认证信息检测装置，以及连接存储有上述用户生物认证信息和决定每个用户访问网络时必要的访问认证信息、具有信号处理功能的外部存储介质，其步骤包括：

将由上述生物认证信息检测装置检测的来自用户的生物认证信息与存储在上述外部存储介质中的生物认证信息进行比较，当两个信息一致时，存储在上述外部存储介质中的上述访问认证信息经由上述用户终端发送给上述管理中心，

在接收到的上述访问认证信息与预先存储的访问认证信息一致的情况下，上述管理中心判断上述用户是注册的正规用户，并许可上述用户终端通过调谐服务器经由上述网络服务社区中的相应代理商连接到上述网络服务社区中的特定网络服务信道。

2．根据权利要求 1 记载的网络访问方法，其特征在于：上述外部存储介质为磁盘，由连接在上述用户终端的磁盘驱动器驱动，该磁盘的电子电路存储上述用户生物认证信息和决定每个用户访问网络时必要的访问认证信息。

3．根据权利要求 1 记载的网络访问方法，其特征在于：上述管理中心具有内置的或与其连接的用户注册中心，在上述用户注册中心存储有上述用户的个人信息和上述访问认证信息。

4．根据权利要求 1 或 3 记载的网络访问方法，其特征在于：上述访问认证信息含有用户的 ID 和密码。

5．根据权利要求 1 或 3 记载的网络访问方法，其特征在于：上述用户在上述管理中心的信息发送接收通过对上述用户预先赋予的昵称进行。

6．根据权利要求 3 记载的网络访问方法，其特征在于：上述访问认证信息被编码后从上述用户终端侧输出，在上述管理中心和用户注册中心，对接收到的编码后的上述访问认证信息进行解码。

7．根据权利要求 6 记载的网络访问方法，其特征在于：上述用户和上述管理中心和用户注册中心之间的信息发送接收是通过使用公开密钥的编码和使用对应于上述公开密钥的秘密解码键的解码处理进行的。

8．根据权利要求 7 记载的网络访问方法，其特征在于：上述访问认证信息在上述用户每次访问时变化，仅上述用户终端和上述管理中心和用户注册中心得知上述变化。

9．根据权利要求 8 记载的网络访问方法，其特征在于：上述用户终端产生上述用户下次访问使用的访问认证信息并对该访问认证信息进行编码后发送到上述管理中心，由管理中心解码后保存，在下次从上述用户终端访问时，上述用户终端发送更新后的上述访问认证信息。

10．根据权利要求 3 记载的网络访问方法，其特征在于：存储在上述管理中心服务器中的与用户有关的个人信息由赋予上述每个用户的基本码管理，确定上述用户的用户个人信息仅通过基本码才可以读取、写入，该基本码是由上述用户终端侧的外部存储介质产生的辅助码和该用户的基础码组合而产生，所述基础码为用户注册中心赋予该用户的唯一编码。

11．根据权利要求 10 记载的网络访问方法，其特征在于：上述基本码由上述用户终端采用管理中心的公开密钥编码后从上述用户终端发送管理中心，在上述管理中心，通过对应于上述公开密钥的秘密解码键解码后作为得到的基本码使用。

12．根据权利要求 1 或 3 记载的网络访问方法，其特征在于：上述用户生物认证信息是指纹认证、容貌认证、声音认证或眼睛的虹膜认证。

13．根据权利要求 2 记载的网络访问方法，其特征在于：上述磁盘是光盘。

根据本发明，存储在光盘（并不局限于光盘的普通磁盘存储介质）的用户个人信息被编码后存储在安装于光盘的电子电路的存储器中，另一方面，在提供服务侧，该用户的个人信息也在被编码后进行保存，由于每一个个人信息可以由只有用户侧和服务提供商侧（网络侧）知道的密钥和解码键进行编码、解码处理，所以安全性显著地提高。即，相对于用户的网络社会，用户持有的光盘具有作为通行证的功能。因此，可以对信息进行限制而仅对用户认为必要的对象提供信息。此外，用户在接受网络服务时（访问网络时），不需要输入用于认证的信息（ID 和密码），由于从被驱动光盘侧自动地产生用于用户认证的信息，所以可以仅在用户侧和服务提供（管理服务器）侧对该信息进行解码，特别是，由于双向发送一次性的密码，所以确保了网络访问时的安全性。可以以用户本人的意思高度安全性地进行服务的加入、归属、退出。并且，由于用户在网络社会公开的不是本人的

姓名而是昵称，所以没有个人信息公开的问题。因此，根据本发明，每个用户通过存储在安装于光盘上的电子电路中的信息访问互联网，所以即使昵称被公开，由于保证了该用户的实际信息，可以接受安全性非常高地互联网的访问及服务。

附图说明

图 1 是根据本发明的网络访问系统的最佳实施例的基本构成的框图。

图 2 是本发明实施例中用光盘驱动器驱动光盘的结构的示意图。

图 3 是表示本发明实施例中登录用户注册中心 4 和管理中心 3 的处理顺序的流程图。

图 4 是表示本发明实施例的用户参加的社会（场、信道）的形成顺序的流程图。

图 5 是表示本发明实施例中在用户的显示器中显示的可以使用的功能和服务内容的示例。

符号说明

1A～1E 用户终端

2A～2E 调谐服务器

3 管理中心

4 用户注册中心

11A～11E 生物认证部

31A～31F 代理商

311～313 信道 CH1～CH3

100 光盘驱动器

110 电子电路

111 发送接收部

112 信号处理部

113 存储器

120 光盘存储器

130 驱动部

140 存储器

200 发送接收装置

300 个人电脑

310 ROM

320 RAM

330 计算处理部

340 显示部

400 生物认证装置

具体实施方式

下面，参照附图详细地说明本发明的网络访问系统、方法以及存储介质的最佳实施例的结构以及动作。图 1 是根据本发明的网络访问系统的一个实施例的基本系统的构成图。

还有，在下面的说明中，虽然使用的是安装有含有 CPU 功能和存储器等的电子电路的光盘，但是显而易见不仅限于光盘，其他任何磁盘、存储介质都适用于本发明。此外，用于实现本发明的结构并不局限于下面描述的结构，可以使用任意公知的结构，可以采用实现同样功能的结构。

图 2 是表示本实施例中用光盘驱动器驱动光盘的结构的图。在图 2 的结构中，使用光盘驱动器 100 使光盘旋转并从光盘读出数据或写入数据。在设置于光盘一面的数据存储部中存储需要的数据（目录等数据）。在与形成有光盘数据存储部的面的相对面安装进行一定信号处理的电子电路（CPU）110。电子电路 110 包括接收发送部 111、信号处理部 112、存储器 113。此外，电子电路 110 的信号处理结果和来自外部的信息，例如，通过光盘驱动器的无线部（发送接收部）111 以无线信号在与外部电路之间发送/接收。

在光盘驱动器 100 中设有插入光盘的插入口（未图示），插入的光盘以一定速度旋转。以光盘的旋转状态，从光学拾波器向光盘表面照射激光，通过借助于光学拾波器检测其反射光读出光学式记录的数据。此外，从光学拾波器照射激光并记录数据。

光盘驱动器 100 包括用于旋转驱动光盘的驱动部 130 和存储器 140（勿庸置疑，这不是必须的）。光盘的一面包括具有写入音乐信息、图像信息、程序信息等数据的 ROM 区域和可以写入任意数据的 RAM 区域中的至少一个的存储部 120，光盘的另一面包括具有 CPU 功能的电子电路 110。例如，电子电路 110 可以作为 RFID（Radio Frequency Identification）部形成。显而易见，也可以在上述一面设置电子电路 110。

通常，RFID 部可以进行使用了电磁波的非接触通信，因此可以以非接触状态对半导体存储器（集成电路芯片）内的数据进行通信（读出写入），通常，RFID 由集成电路芯片和与其连接的线圈状天线构成。

接收发送装置 200 具有读写功能，在作为设置在上述光盘面上的电子电路 110 的 RFID 部的集成电路芯片内的接收发送部 111 之间通过无线通信进行数据发送接收。发送接收装置 200 与电子电路 110 的发送接收部 111 之间的数据通信是以例如 106kbps 的传输

速度进行的。

电子电路 110（RFID 部）内的天线（发送接收部 111）当接收来自发送接收装置 200 的电波时，由于共振作用产生电动势（电磁感应等），所以通过电源整流部对该电动势进行整流并作为电子电路 110 的电源使用。通过该电源启动 RFID 部内的集成电路芯片。

勿庸置疑，电源供给并不局限于这种结构。

个人电脑 300 包括存储 OS 等基本信息的 ROM（存储装置）310、作为可擦写的存储部的 RAM320、CPU 等的演算处理部 330、液晶显示器等的显示部 340，个人电脑 300 与光盘驱动器 100 之间进行数据接收发送，进行所需信号的处理。

生物认证装置 400 由于仅限于许可本系统的启动、动作的用户，所以考虑指纹认证、容貌认证、声音认证、眼睛的虹膜认证等的生物类参数。在光盘驱动器 100 启动时（事先连接于个人电脑 300 上，在它启动时也同样），例如，使用户将一定的手指接触在生物认证装置 400 的用于指纹认证的指纹读取部，进行光学读取，并与预先存储、注册的用户的指纹进行核对，仅有当两者一致时，才认为是正规的用户，准许使用。

那么，以如上所述的结构为前提，在本实施例中，采用防止由于非法假冒导致的入侵和个人信息泄漏的各种方案。

首先，给每个用户准备安装了含有存储器的电子电路 110 的光盘，或者为希望使用的用户每次加入社区准备安装了含有存储器的电子电路 110 的光盘。在电子电路 110 的存储器中存储有用户 ID 和访问时必要的信息。这些信息（例如 ID、密码等）根据用户的每一次访问产生变化，以及这些信息被事先进行了编码处理，只有用户和设置于服务提供侧的管理中心侧才可以得知。在电子电路的存储器中还存储有用于用户认证的认证信息。在本实施例中，存储有例如指纹数据的生物认证数据。

在光盘驱动装置 100，与作为生物认证装置 400 的指纹检测装置连接（或内置于其中），当用户将自己的光盘插入光盘驱动装置中时，光盘驱动装置将通过指纹检测装置得到的指纹数据与存储在光盘的电子电路的存储器中的指纹数据进行核对，当判断两者一致时，判断为正规的用户，进行接下来的处理步骤。

当参照图 1 时，本实施例的预先注册的一个或多个用户 A～D 使用各自使用的个人电脑等的用户终端 1A～1D（图 2 的个人电脑 300）、……,例如通过互联网等网络参加作为服务提供者的管理中心 3 管理的社区的情况是适用了本发明的实施例。

在管理中心 3 管理的社区中，设置有多个社会（图中是信道（CH1～CH3））311～313，用户通过调谐服务器 2A～2D……等向管理中心 3 要求加入、参加自己希望的社会。

在本实施例中采用的结构，用户预先在运行管理中心 3 的组织（用户注册中心 4）中

注册，仅注册过的用户可以接受管理中心 3 管理的网络服务（参加社会等）。即，被赋予了已注册用户的用户码 ID、密码 PW 等的用户向管理中心 3 发出这些信息，仅由管理中心 3 侧认定为已正规注册的用户才可以访问并享受上述服务。

管理中心 3 具有多个代理商（Ag）31A～31E……，控制外部（调谐服务器等）与社会（信道 CH1（311）、CH2（312）、CH3（313）……）的连接。在图 1 中，在各个用户终端 1A～1E 中设有对应的代理商 31A～31E。

管理中心 3 内部安装有用户注册中心 4 或通过代理商 31F 连接于用户注册中心 4，在该用户注册中心中存储用户信息。用户注册中心 4 对作为用户信息的个人信息、ID 信息、密码（PW）等进行必要的编码后进行存储、管理。例如，用户 A～E 的驾驶执照、居民身份证等的个人信息由各个编码键（UAI1～UEI1）进行编码并存储在存储器中，此外，管理分配给每个用户的识别 ID 和密码 PW。这里，U 表示用户，A、E 表示各个用户，I 表示个人信息，最后的数字表示第几次访问、处理的数字。

用户注册中心 4 管理各种信息，管理用户 A～E 的密码 PW1、PW2、ID 信息（ID0、AIDi）、管理中心 3 的密码 KApi 的管理、信道和代理商的管理、公开密钥 Ke 和秘密解码键 Kd 等各种信息。用户注册中心 4 通过代理商 31F 连接到管理中心 3，进行信息的接收发送。

调谐服务器 2A～2E 连接到代理商 31A～31F，通过这些代理商，直接地进行相互连接时所期望的与调谐服务器的连接。其与在连接时使用两者的 IP 地址的通过 IP 网络进行连接的通常的互联网连接不同。

在以上的结构中，在用户终端 1A～1E 和管理中心 3（用户注册中心 4）之间进行信号的发送接收时，为了确保安全性，进行各种编码处理和解码处理。该编码通过公开密钥进行。解码处理通过与公开密钥对应的密码解码键进行。

接下来，针对本实施例中用户信息的用户注册中心 4 和管理中心 3 的注册处理，特别是对社会的加入形成处理进行说明。

首先，对这些处理中使用的符号的意义进行说明。（这里，针对用户 A 进行说明）。

Ae[ID0,Ap0,AI0]表示由公开密钥 Ae 对用户 A 的第“0”个（最初）ID（ID0：基础码）、密码（Ap0）以及密钥（AI0）的信息进行编码后的信息。

此外，Ad{ Ae[ID0,Ap0,AI0]}表示由密码解码键 Ad 对上述 Ae[ID0,Ap0,AI0]进行解码后的信息。

Ke 和 Kd 表示由管理中心 3 管理的公开密钥和秘密解码键，预先由管理中心 3 事先生成。用户注册中心 4 的公开密钥 Ue 和秘密解码键 Ud 也同样事先生成。

UAI0 是由用户注册中心 4 发行的用户 A 的初始密钥，用户注册中心 4 利用用户 A 的初始密钥 UAI0 对用户 A 的个人信息进行编码，并由预先赋予了如后所述的基础码 ID0 的标识符的持有者存储、管理。

基础码 ID0 是用户注册中心 4 发行的唯一存在的唯一码，例如分配 P4KYU%7 这样的唯一码。实际上，给基础码 ID0 分配的是假定为唯一的码。用户注册中心 4 利用基础码 ID0 管理用户的个人信息，根据该基础码 ID0 进行信息的读出、写入。但是，用户注册中心 4 仅可以管理对应于基础码 ID0 的信息，不能得到确定用户本人的信息。

Kd{Ke[ID0,Ap0]}表示由管理中心 3A 的公开密钥 Ke 对[ID0,Ap0]进行编码后的信息 Ke[ID0,Ap0]是通过管理中心 3 的秘密解码键 Kd 进行解码后的信息。

Ad{Ae[ID0,Ap0]}表示由用户 A 的公开密钥 Ae 对[ID0,Ap0]进行编码后的信息 Ae[ID0,Ap0]是通过用户的秘密解码键 Ad 进行解码后的信息。

AID1 称为基本码，由基础码 ID0 和辅助码 AAID1 构成，由 AID1＝ID0（基础码）＋AAID1（辅助码）表示，辅助码 AAID1 由安装在用户所有的光盘上的电子电路产生。

不通过基本码就无法获得用户 A 的信息（不局限于个人信息的所有必要信息）。即，单独通过基础码 ID0 或辅助码 AAID1，不能访问确定用户 A 的信息，只有通过两者齐备的基本码 AID1 才可以访问。因此，如前所述，在用户注册中心 4 不能访问确定用户 A 的信息。

例如可以用 OP4KYU%7 表示基础码 ID0，用 QSC56VBA 表示辅助码 AAID1，则基本码 AID1 可以如下表示：

AID1＝OP4KYU%7＋QSC56VBA。

Ud{ Ue[ID0,UAI1,Ap1]}表示由用户注册中心 4 的公开密钥 Ue 对（ID0,UAI1,Ap1）编码后的信息是通过秘密解码键 Ud 进行解码的信息。

Ke[ID0，AID1，Ap1，昵称]表示由管理中心 3 的公开密钥 Ke 对（ID0，AID1，Ap1，昵称）进行编码的信息。

Kd{ Ke[ID0，AID1，Ap1，昵称]}表示由管理中心 3 的公开密钥 Ke 对（ID0，AID1，Ap1，昵称）进行编码的信息是通过管理中心 3 的密码解码键 Kd 进行解码的信息。

接下来，参照图 3 的流程图针对用户注册中心 4 和管理中心 3 的注册处理进行说明。

首先，用户向用户注册中心 4 出示可以证明身份的驾驶执照、居民身份证等资料（步骤 S101）。用户注册中心 4 利用用户 A 的公开密钥（Ae）对作为用户信息的 ID（ID0：基础码）和密码 PW1（Ap0：用户 A 的初始密码）和初始密钥（AI0）进行编码，在安装在用户 A 的光盘中的电子电路中进行注册（步骤 S102）的同时，由用户注册中心 4 的初

始密钥 UAI0 对驾驶执照、居民身份证等的个人信息进行编码并注册、存储在服务器（存储器）中（步骤 S103）。

用户注册中心 4 还使用由管理中心 3 准备的公开密钥 Ke 对用户 A 的信息 ID（ID0）和密码 PW1（Ap0）进行编码，并发送到管理中心 3（步骤 S104）。

管理中心 3 使用管理中心 3 准备的秘密解码键 Kd 对从用户注册中心 4 接收的信息 ID（ID0）和密码 PW1（Ap0）进行解码并保存，同时，产生管理中心 3 的密码 PW2（KAp0）（步骤 S105）。

还有，实际上，用户 A 访问时，打开个人电脑和外围设备的电源，使用生物认证装置 11A（图 2 中为生物认证装置 400）进行生物认证，确认是正确的用户后，启动光盘（步骤（S106），并启动安装在光盘或个人电脑中的调谐服务器 2A（步骤 S107）。

接下来，电子电路使用预先准备的密码解码键 Ad 对在用户注册中心 4 中注册于光盘的 ID（基础码 ID0）和密码 PW1（Ap0）进行解码并确认（步骤 S108）。此外，电子电路产生辅助码（AAID1），与在光盘中注册的基础码 ID0 相加，产生基本码 AID1（AID1＝ID0＋AAID1）（步骤 S109）。此时，电子电路根据由用户注册中心 4 注册的初始密钥 UAI0,产生用于用户注册中心 4 编码的用户 A 的密钥 UIAI1、密钥 AI1 以及密码 PW(Ap1)（步骤 S110）。用户终端 1A 的电子电路产生用户 A 的公开密钥 Ae、秘密解码键 Ad、密码 PW1、管理中心 3 使用的密码 PW2、ID（基本码 AID1）、密码 AIi 等信息。其它用户终端 1B～1E 也产生同样的信息。

用户终端 1A 使用用户注册中心 4 的公开密钥（Ue）对基础码 ID0、密钥 UAI1、密码 PW（Ap1）进行编码，并发送到用户注册中心 4（步骤 S111）。

用户注册中心 4 使用准备好的秘密解码键 Ud 对接收到的信息进行解码，并且在读入赋予基础码 ID0 的标识符的持有者的个人信息且使用对应于密钥 UAI0 的解码键进行解码后，由密钥 UAI1 进行编码，并更新、保存。此外，密码 PW（Ap1）也由同样的持有者更新、保存（步骤 S112）。

用户终端 1A 通过管理中心 3 的公开密钥（Ke）对作为访问码的基础码 ID0、基本码 AID1、密码 PW（Ap1）、任意赋予用户 A 的昵称进行编码，并发送到管理中心 3（步骤 S113）。

管理中心 3 使用准备好的秘密解码键 Kd 对从用户终端 1A 接收的信息进行解码，由基础码 ID0 对应的持有者保存（步骤 S114）：

（1） 用户 A 更新后的基本码 AID1

（2） 用户 A 更新后的密码 PW（Ap1）

（3） 从管理中心发送到用户 A 的密码 PW（KAp0）

（4） 用户 A 的昵称。

步骤S110处理后，在安装于用户终端1A侧的光盘中的电子电路中保存（步骤S115）：

（1） 由 AI1 再次编码的驾驶执照、居民身份证等个人信息

（2） 由 AI1 编码后的基础码 ID0 和 AID1

（3） 由 AI1 编码后的密码 PW（Ap1）

（4） 由 AI1 编码后的来自管理中心 3 的密码 PW（Kap0）

（5） 用户 A 的昵称

（6） 用户注册中心 4 的密钥 UAI1。

步骤 S112、S114 以及 S115 的处理后，以下，利用用户 A 的光盘的电子电路对第 i 个编码键、基本码、密码：UAIi、AIDi、PW（Api）逐个进行更新，同时，由管理中心 3 以及用户注册中心 4 的 ID0 的持有者存储的信息也逐个进行更新（步骤 S116）。

如上述说明的，本实施例如此构成：在访问互联网时，二维地自动产生必要的用户 ID 和密码，而且在下一次访问时，每次变化地产生 ID 和密码。产生的 ID 和密码可以被编码，也可以仅被分别解码。

接下来，参照图 4 的流程图说明社会（场、信道）的形成处理。

首先，用户 A 打开个人电脑和外围设备的电源，使用指纹认证装置 11A 进行生物认证，当确认是正规的用户时，使用光盘驱动器启动光盘（步骤 S201），并启动调谐服务器 2A（步骤 S202）。该调谐服务器 2A 是通过在光盘中安装（设定）的、以用户为单位设定的特殊程序进行处理的，可以作为用于网络连接的特定程序。该特定程序是根据预先存储在光盘中的用户特有的信息实行设置在服务提供侧的管理中心 3 中的、用于进行与用户希望的社会(场、信道：CH1、CH2、CH3、……)连接的处理的程序。

即，用户终端 1A 使用对应于密钥 AI1 的解码键对在用户注册中心 4 注册于光盘的 ID（基本码 AID1）、密码 PW（Ap1）进行解码，并同时使用管理中心 3 的公开密钥 Ke 对其所属的信道（在本实施例中是信道 CH1）进行编码并发送（步骤 S203）。调谐服务器（FS）2A 将从用户终端 1A 接收的信息传送到对与社会的连接进行控制的代理商 31A（步骤 S204），代理商 31A 将其发送到管理中心 3（步骤 S205）。

管理中心 3 使用秘密解码键 Ke 对希望信道（CH1）、密钥 AI1、基本码 AID1 以及密码 Ap1 进行解码（步骤 S206）。用户终端 1A 使用解码（秘密）键 Ad 对由管理中心 3 侧的用户 A 的密钥编码后的基本码 AID1 以及密码的初始值 Ap0 进行解码并得到基本码 AID1 和管理中心 3 侧的密码 KAp0（步骤 S207）。

接下来，将如此得到的用户 A 的 ID 和密码 PW 进行比较（步骤 S208），如果不一致，管理中心 3 要求用户 A 再次发送 ID 和密码 PW（步骤 S209），管理中心 3 要求将由用户 A 的公开密钥 Ae 编码后的基本码 AID1 和管理中心 3 的用户 A 的密码 PW（KAp0）一起添附后，再传送至用户终端 1A 的电子电路（步骤 S210）。

于是，用户 A 使用秘密解码键 Ad 对基本码 AID1 和管理中心 3 的密码 KAp0 进行解码并获得，将基本码 AID1 和管理中心 3 的密码 KAp0 与用户 A 具有的码进行比较，认证其是来自管理中心 3（步骤 S211）。此后，返回步骤 S203 的处理。

当判断步骤 S208 中的比较结果、ID 和密码 PW 两者一致时，通过用户 A 的 ID（AID1）和密码 PW（Ap1）认证用户 A，管理中心 3 命令代理商 31A 以使连接用户 A 想要的信道 CH1（步骤 S212）。

代理商 31A 通过代理商 31A 连接用户 A 的调谐服务器（FS）2A 和信道 CH1（步骤 S213）。

同样地，用户终端 1B 和 1C 等也连接希望的用户终端，形成信道 CH1 的社会（步骤 S214）。

安装在用户终端 1A 的光盘中的电子电路产生新的（第二次访问）密码 Ap2 和密钥 AID2，同时使用管理中心 3 的公开密钥 Ke 对 ID0 进行编码并发送（步骤 S215）。

管理中心 3 产生密码 KAp1，利用用户 A 的公开密钥 Ae 对产生的密码 KAp1 进行编码并发送给用户终端 1A（步骤 S216）。用户 A 接受社会的通信、服务（步骤 S217），服务结束后，用户 A 向代理商 31A 要求断开（步骤 S218）。

步骤 S218 的处理后，利用用户 A 的 ID（ID1）和密码 PW（Ap1）认证用户 A，认证时，管理中心 3 命令代理商 31A 断开用户 A 希望的信道 CH1（步骤 S221）。管理中心 3 将用户 A 的 ID 更新为新产生的基本码 AID2，将密码 PW 更新为新产生的密码 Ap2，并保存(步骤 S222)。并且，代理商 31A 断开用户 A 的调谐服务器（FS）2A 和信道（CH1）（步骤 S223）。

另一方面，在步骤 S215 的处理之后，对于用户注册中心 4 使用公开密钥 Ue 对用户 A 的第二次访问时的密码 Ap2 和基础码 ID0 进行编码并发送给用户注册中心 4（步骤 S219），用户注册中心 4 更新并保存使用秘密解码键 Ud 解码并得到的密码 Ap2（步骤 S220）。

经过与以上相同的处理连接其他用户的任意信道，接受期望服务的提供。

这样多个用户可以参加一定的社会。在参加到社会的用户（A）使用的个人电脑的显示器的画面中，显示出参加的社会公告板，显示含有用户 A 的参加用户的昵称。此外，在

同一个公告板上，如图 5 所示，显示用户（A）可以使用的（读取、写入）功能和服务（聊天、电话、主页、问卷调查等）。

在本实施例中，由于需要相互连接的调谐服务器不经过 IP 网络或电子邮件地址而直接连接，所以不会公开这些个人信息，可以从电子邮件杂志服务提供商设置的用户终端接收电子邮件杂志等。

此外，如果将用户终端设置在银行或运营商侧，可以在网上购物后，通过给银行侧的终端输入账户转帐指令，则可以在不向商家公开信用卡信息的情况下完成上述转帐行为，所以可以对运营商仅公开住址，良好地避免了个人信息的无限制公开，提高安全性。

勿庸置疑，上述实施例中的各个处理作为程序被描述，可以根据该程序由计算机实现该处理，该程序存储在存储介质中。

以上，详细地描述了本发明最佳实施例的结构和操作。但是，这些实施例仅仅是本发明的示例，并不是对本发明进行限定。本领域的技术人员可以理解，在不偏离本发明宗旨的情况下，可以根据特定用途进行各种修改和变化。例如，毫无疑问，电子电路也可以是光学电路，信息可以存储在电子电路中和/或存储在磁盘中。此外，毫无疑问，也可以使用诸如 USB 存储器这种从外部连接的可移动的存储介质代替磁盘。

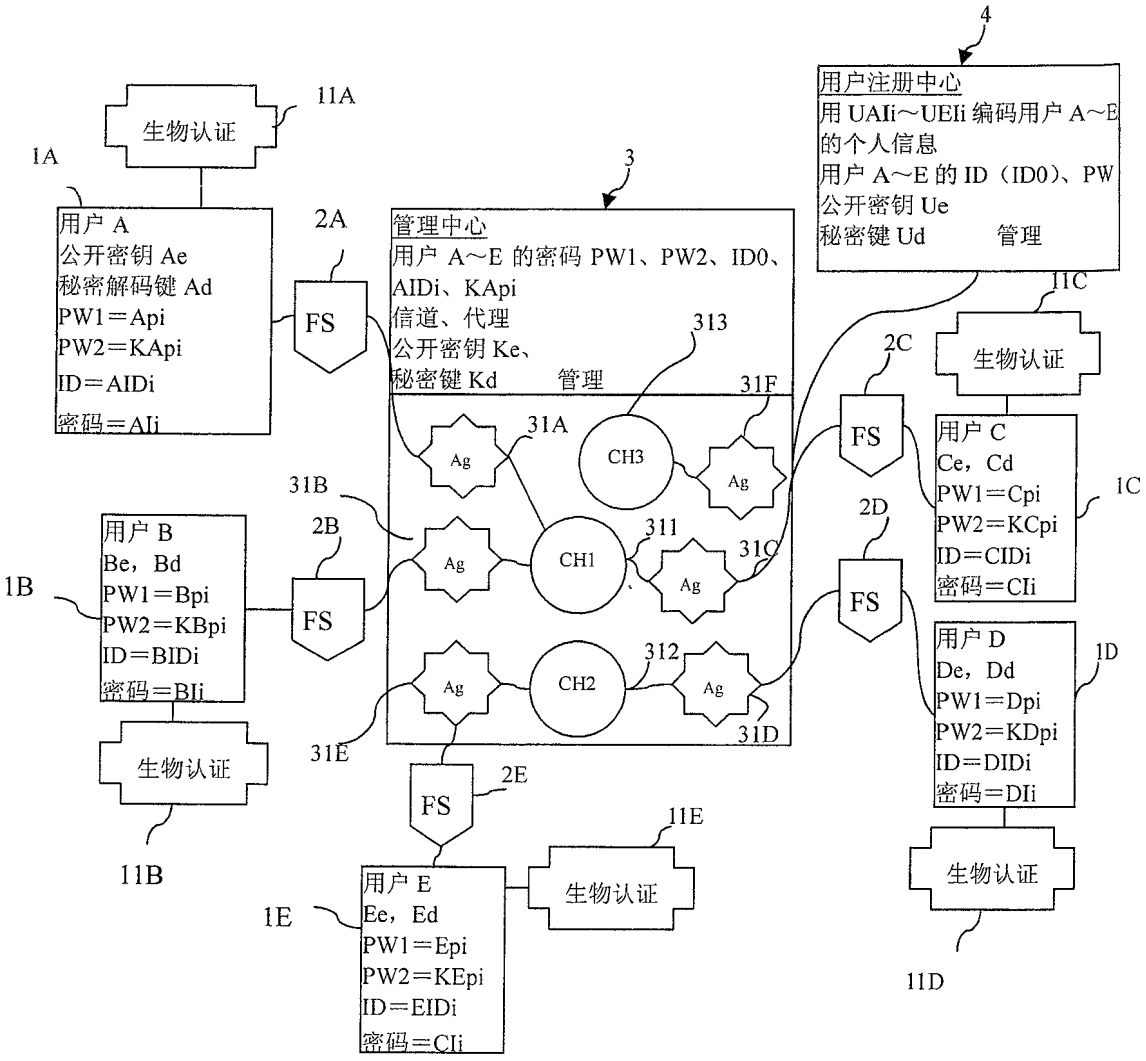

4
用户注册中心
用 UAIi～UEIi 编码用户 A～E 的个人信息
用户 A～E 的 ID（ID0）、PW
公开密钥 Ue
秘密键 Ud 管理
11A
生物认证
1A
用户 A
公开密钥 Ae
秘密解码键 Ad
PW1＝Api
PW2＝KApi
ID＝AIDi
密码＝AIi
2A
FS
3
管理中心
用户 A～E 的密码 PW1、PW2、ID0、AIDi、KApi
信道、代理
公开密钥 Ke、
秘密键 Kd 管理
313
31F
31A
Ag
CH3
Ag
11C
生物认证
2C
FS
用户 C
Ce，Cd
PW1＝Cpi
PW2＝KCpi
ID＝CIDi
密码＝CIi
1C
31B
2B
1B
用户 B
Be，Bd
PW1＝Bpi
PW2＝KBpi
ID＝BIDi
密码＝BIi
Ag
CH1
311
31C
Ag
FS
2D
FS
用户 D
De，Dd
PW1＝Dpi
PW2＝KDpi
ID＝DIDi
密码＝DIi
1D
312
Ag
CH2
Ag
31E
31D
2E
FS
11E
生物认证
11B
生物认证
1E
用户 E
Ee，Ed
PW1＝Epi
PW2＝KEpi
ID＝EIDi
密码＝CIi
生物认证
11D

图 1

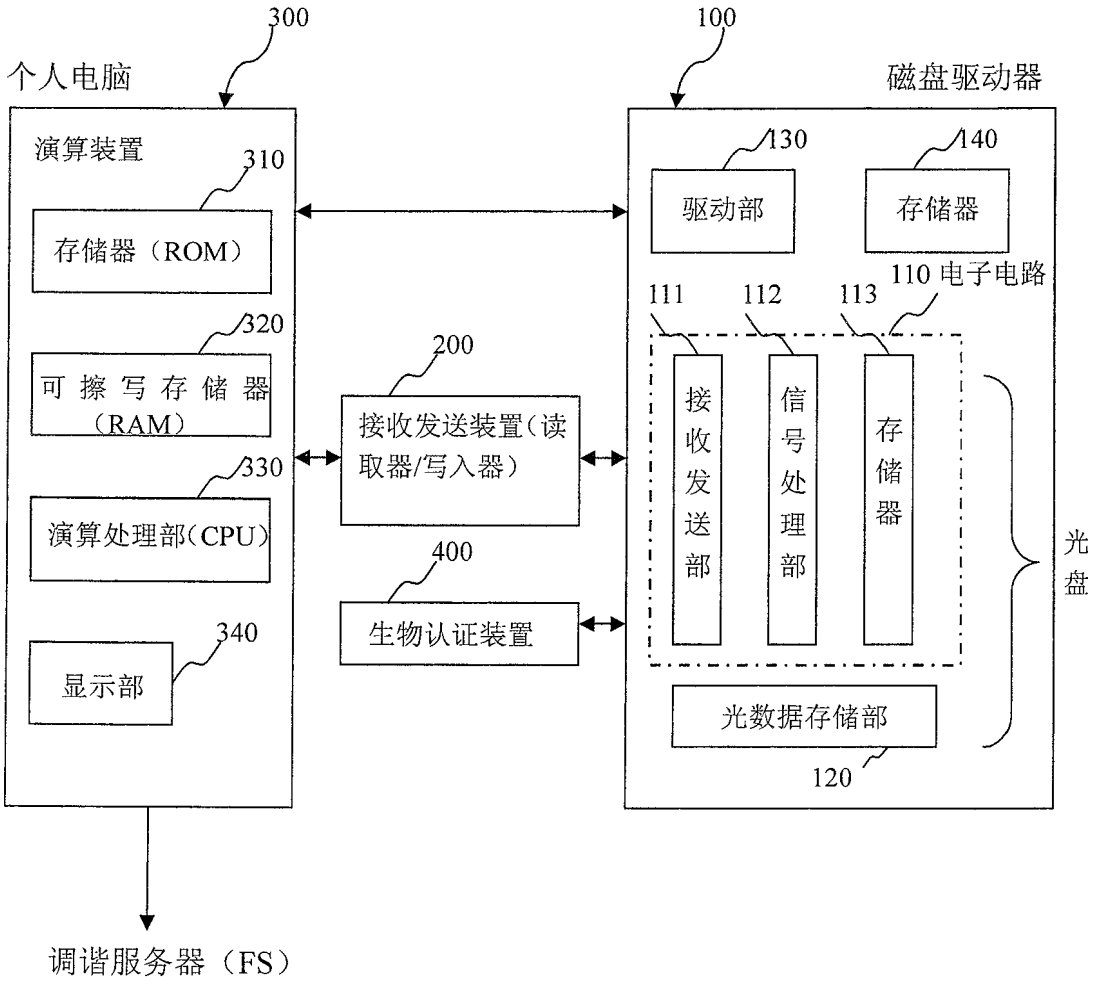

300
个人电脑
演算装置
310
存储器（ROM）
320
可擦写存储器（RAM）
330
演算处理部(CPU)
340
显示部
调谐服务器（FS）
200
接收发送装置(读取器/写入器)
400
生物认证装置
100
磁盘驱动器
130
驱动部
140
存储器
110 电子电路
111
112
113
接收发送部
信号处理部
存储器
光盘
光数据存储部
120

图 2

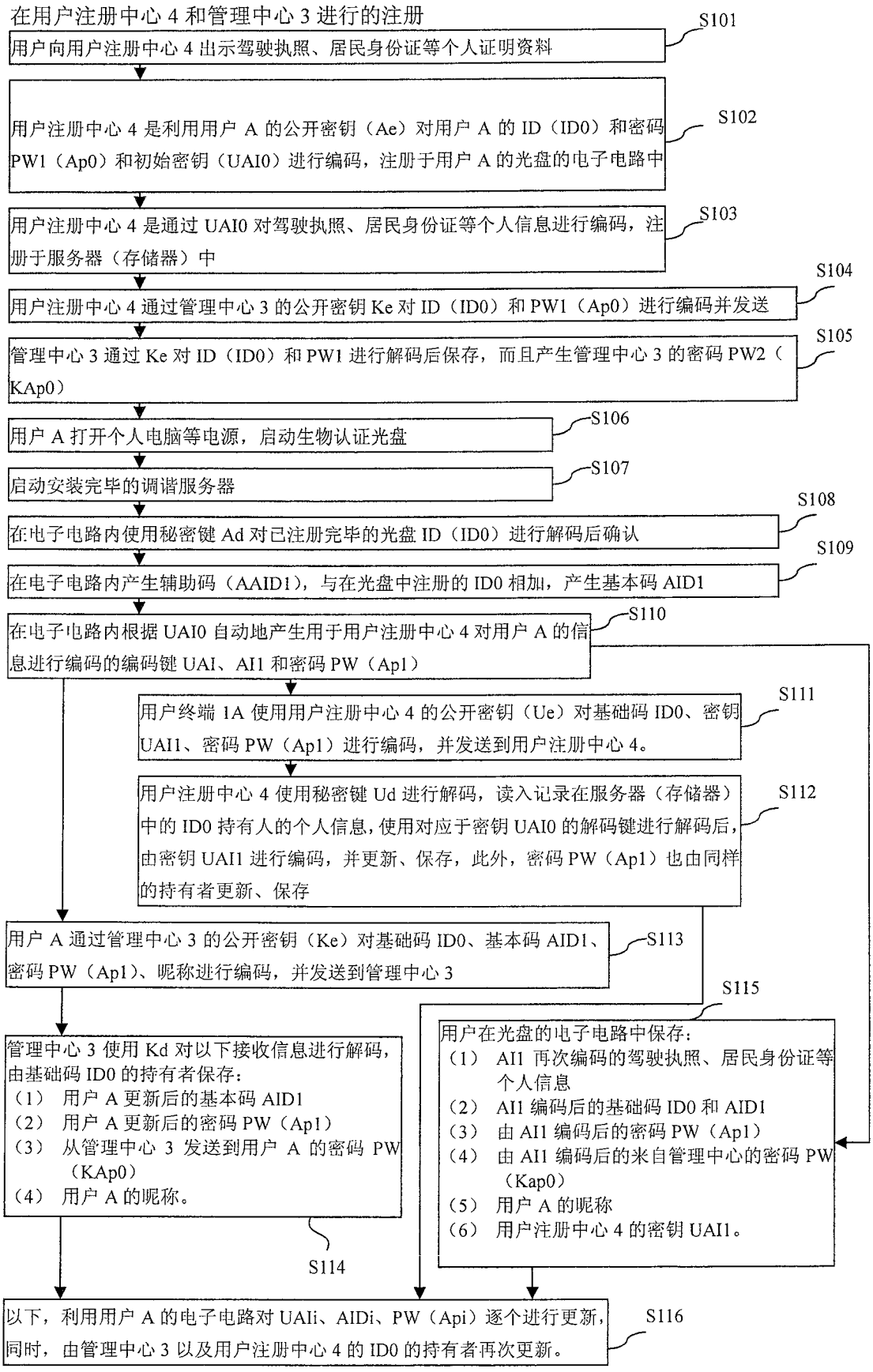

在用户注册中心 4 和管理中心 3 进行的注册
S101
用户向用户注册中心 4 出示驾驶执照、居民身份证等个人证明资料
用户注册中心 4 是利用用户 A 的公开密钥（Ae）对用户 A 的 ID（ID0）和密码 PW1（Ap0）和初始密钥（UAI0）进行编码，注册于用户 A 的光盘的电子电路中
S102
用户注册中心 4 是通过 UAI0 对驾驶执照、居民身份证等个人信息进行编码，注册于服务器（存储器）中
S103
用户注册中心 4 通过管理中心 3 的公开密钥 Ke 对 ID（ID0）和 PW1（Ap0）进行编码并发送
S104
管理中心 3 通过 Ke 对 ID（ID0）和 PW1 进行解码后保存，而且产生管理中心 3 的密码 PW2（KAp0）
S105
用户 A 打开个人电脑等电源，启动生物认证光盘
S106
启动安装完毕的调谐服务器
S107
在电子电路内使用秘密键 Ad 对已注册完毕的光盘 ID（ID0）进行解码后确认
S108
在电子电路内产生辅助码（AAID1），与在光盘中注册的 ID0 相加，产生基本码 AID1
S109
在电子电路内根据 UAI0 自动地产生用于用户注册中心 4 对用户 A 的信息进行编码的编码键 UAI、AI1 和密码 PW（Ap1）
S110
用户终端 1A 使用用户注册中心 4 的公开密钥（Ue）对基础码 ID0、密钥 UAI1、密码 PW（Ap1）进行编码，并发送到用户注册中心 4。
S111
用户注册中心 4 使用秘密键 Ud 进行解码，读入记录在服务器（存储器）中的 ID0 持有人的个人信息，使用对应于密钥 UAI0 的解码键进行解码后，由密钥 UAI1 进行编码，并更新、保存，此外，密码 PW（Ap1）也由同样的持有者更新、保存
S112
用户 A 通过管理中心 3 的公开密钥（Ke）对基础码 ID0、基本码 AID1、密码 PW（Ap1）、昵称进行编码，并发送到管理中心 3
S113
管理中心 3 使用 Kd 对以下接收信息进行解码，由基础码 ID0 的持有者保存：
（1） 用户 A 更新后的基本码 AID1
（2） 用户 A 更新后的密码 PW（Ap1）
（3） 从管理中心 3 发送到用户 A 的密码 PW（KAp0）
（4） 用户 A 的昵称。
S114
S115
用户在光盘的电子电路中保存：
（1） AI1 再次编码的驾驶执照、居民身份证等个人信息
（2） AI1 编码后的基础码 ID0 和 AID1
（3） 由 AI1 编码后的密码 PW（Ap1）
（4） 由 AI1 编码后的来自管理中心的密码 PW（Kap0）
（5） 用户 A 的昵称
（6） 用户注册中心 4 的密钥 UAI1。
以下，利用用户 A 的电子电路对 UAIi、AIDi、PW（Api）逐个进行更新，同时，由管理中心 3 以及用户注册中心 4 的 ID0 的持有者再次更新。
S116

图 3

社会（场、信道）的形成

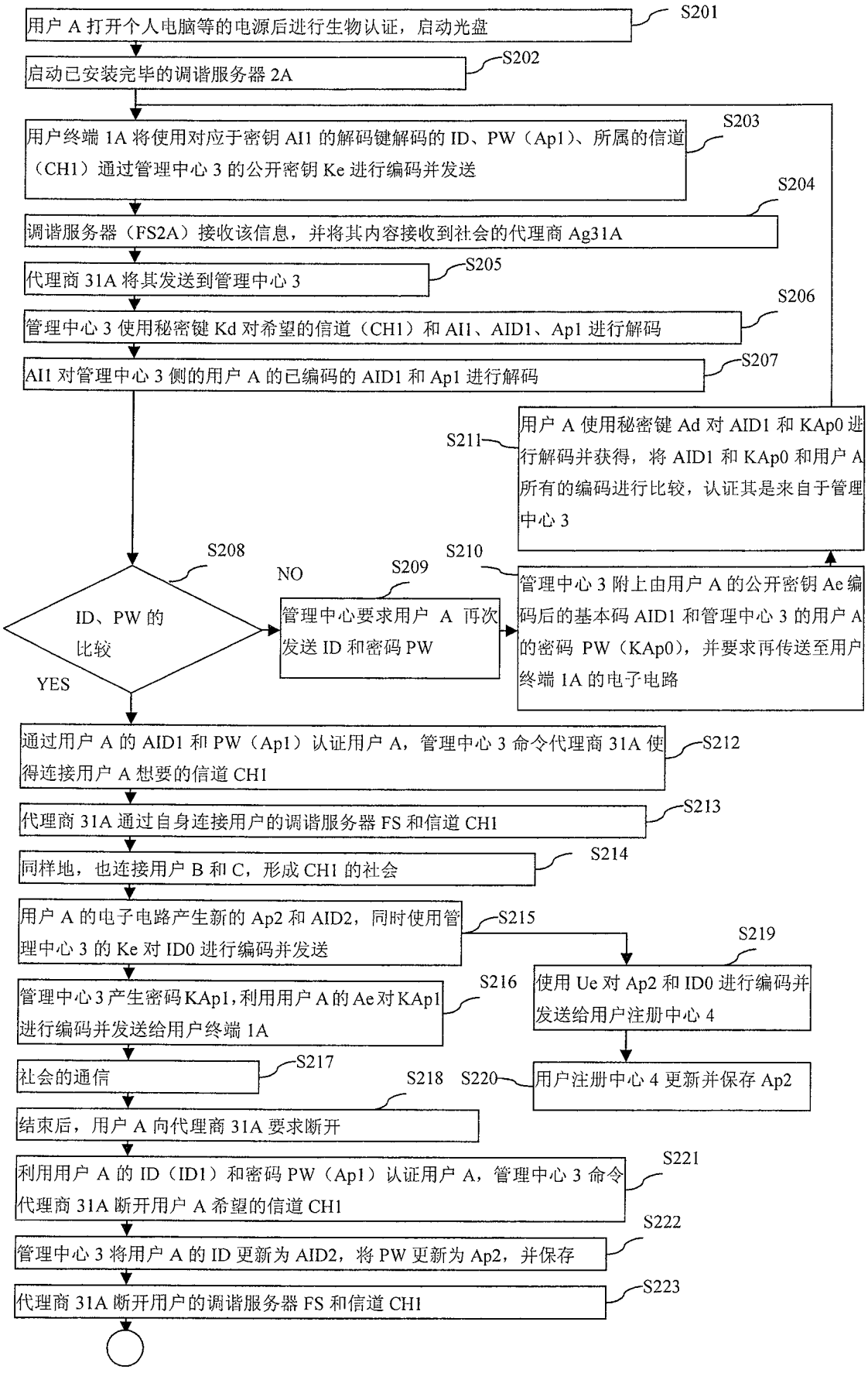

用户 A 打开个人电脑等的电源后进行生物认证，启动光盘
S201
启动已安装完毕的调谐服务器 2A
S202
用户终端 1A 将使用对应于密钥 AI1 的解码键解码的 ID、PW（Ap1）、所属的信道（CH1）通过管理中心 3 的公开密钥 Ke 进行编码并发送
S203
调谐服务器（FS2A）接收该信息，并将其内容接收到社会的代理商 Ag31A
S204
代理商 31A 将其发送到管理中心 3
S205
管理中心 3 使用秘密键 Kd 对希望的信道（CH1）和 AI1、AID1、Ap1 进行解码
S206
AI1 对管理中心 3 侧的用户 A 的已编码的 AID1 和 Ap1 进行解码
S207
用户 A 使用秘密键 Ad 对 AID1 和 KAp0 进行解码并获得，将 AID1 和 KAp0 和用户 A 所有的编码进行比较，认证其是来自于管理中心 3
S211
ID、PW 的比较
S208
NO
管理中心要求用户 A 再次发送 ID 和密码 PW
S209
管理中心 3 附上由用户 A 的公开密钥 Ae 编码后的基本码 AID1 和管理中心 3 的用户 A 的密码 PW（KAp0），并要求再传送至用户终端 1A 的电子电路
S210
YES
通过用户 A 的 AID1 和 PW（Ap1）认证用户 A，管理中心 3 命令代理商 31A 使得连接用户 A 想要的信道 CH1
S212
代理商 31A 通过自身连接用户的调谐服务器 FS 和信道 CH1
S213
同样地，也连接用户 B 和 C，形成 CH1 的社会
S214
用户 A 的电子电路产生新的 Ap2 和 AID2，同时使用管理中心 3 的 Ke 对 ID0 进行编码并发送
S215
管理中心 3 产生密码 KAp1，利用用户 A 的 Ae 对 KAp1 进行编码并发送给用户终端 1A
S216
使用 Ue 对 Ap2 和 ID0 进行编码并发送给用户注册中心 4
S219
社会的通信
S217
用户注册中心 4 更新并保存 Ap2
S220
结束后，用户 A 向代理商 31A 要求断开
S218
利用用户 A 的 ID（ID1）和密码 PW（Ap1）认证用户 A，管理中心 3 命令代理商 31A 断开用户 A 希望的信道 CH1
S221
管理中心 3 将用户 A 的 ID 更新为 AID2，将 PW 更新为 Ap2，并保存
S222
代理商 31A 断开用户的调谐服务器 FS 和信道 CH1
S223

图 4

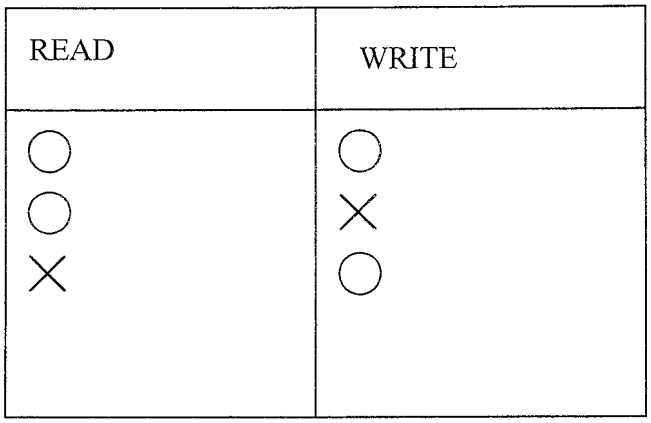


图 5