[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04M 15/00

[12] 发明专利说明书

[21] ZL 专利号 96111183.6

[45] 授权公告日 2004 年 4 月 21 日

[11] 授权公告号 CN 1147120C

[22] 申请日 1996.9.5 [21] 申请号 96111183.6

[30] 优先权

[32] 1995. 9. 5 [33] JP [31] 227843/1995

[71] 专利权人 佳能株式会社

地址 日本东京

[72] 发明人 岩村惠市

审查员 李婷婷

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

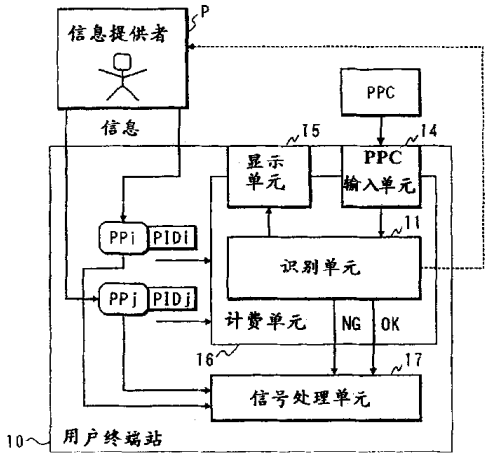
代理人 杜日新

权利要求书 2 页 说明书 21 页 附图 6 页

[54] 发明名称 费用计算装置、信息接收装置和通信系统

[57] 摘要

提供了一种通信系统和费用计算装置，可以容易地管理在多媒体网络中用户使用信息的费用计算并同时能为用户保密。当用户向用户终端的 PPC 输入单元输入钱信息时(钱信息包括现金，预付卡，IC 卡之类)，识别单元按照由钱信息指示的钱数与/或附加于由信息提供者提供的信息上的费用信息判断被提供的信息是否允许使用。响应使用允许信号，信号处理单元处理所提供的信息并将其供给用户。



ISSN1008-4274

1. 一种费用计算装置，该装置包括：

输入装置，用于输入表示金钱的金额的金额信息；

允许信号输出装置，用于判断输入的金额信息和通过网络由提供者终端提供的电子信息的使用费用，以及根据该判断，输出允许信号以允许电子信息的使用；

信息处理装置，用于在所述输出装置输出允许信号的情况下、执行处理以使得能够得到所述电子信息，在所述输出装置不输出允许信号的情况下，不执行所述处理；以及

输出装置，用于输出执行了所述处理的电子信息。

2. 一种费用计算方法，该方法包括：

输入步骤，用于输入表示金钱的金额的金额信息；

允许信号输出步骤，用于判断输入的金额信息和通过网络由提供者终端提供的电子信息的使用费用，以及根据该判断，输出允许信号以允许电子信息的使用；

信息处理步骤，用于在所述输出步骤输出允许信号的情况下、执行处理以使得能够得到所述电子信息，在所述输出步骤不输出允许信号的情况下，不执行所述处理；以及

输出步骤，用于输出执行了所述处理的电子信息。

3. 如权利要求 2 所述的费用计算方法，其中所述电子信息是加密的，并且所述信息处理执行对所述电子信息解码的处理。

4. 如权利要求 2 所述的费用计算方法，其中在所述输入步骤输入的所述金额信息表示现金。

5. 如权利要求 2 所述的费用计算方法，其中在所述输入步骤输入的所述金额信息表示记录在记录介质中的金钱的金额。

6. 如权利要求 2 所述的费用计算方法，其中所述电子信息的使用费用是利用所述电子信息通过网络由所述提供者终端提供的。

7. 如权利要求 2 所述的费用计算方法，还包括传输有关所述电

子信息的使用状态的信息的步骤。

8. 一种信息提供系统，包括：

提供者终端，用于提供电子信息；

用户终端，用于使用通过网络从所述提供者终端接收的所述电子信息；

收费装置，用于输入表示金钱金额的金额信息；

判断装置，用于判断在所述收费装置输入的金额信息和所述电子信息的使用费用，以及根据该判断，输出允许信号以允许电子信息的使用；

信息处理装置，用于在所述判断装置输出允许信号的情况下、执行处理以使得能够得到所述电子信息，在所述判断装置不输出允许信号的情况下，不执行所述处理；以及

输出装置，用于输出执行了所述处理的电子信息。

费用计算装置、信息接收装置和通信系统

技术领域

本发明涉及一种费用计算装置、信息接收装置以及用于多媒体之类的网络中的通信系统，其中所传输的信息包括运动图象数据、静止图象数据、声音数据、计算机数据、计算机程序等，并且本发明的特征在于信息的提供及其费用计算系统。

背景技术

在中继通信网络领域中，光纤网络已经成熟了，已经研制出了有线电视系统，卫星通信已付诸实用，局部区域网络已经普及，通过使用这种通信网络提供各种信息。信息服务业务的规模不断扩大，它们按照信息的数量和内容收费。对于这种业务，合适地收取所提供的信息的费用是重要的。

信息保护仍不完善，因而存在非法使用信息的问题，其中包括程序、图象和声音。为了避免非法使用，提供了复制保护功能，进行序列号检查或采用其它方法。在序列号检查中，当每个程序被执行时，硬件序列号和软件序列号相互比较。当要进行备份时，复制保护功能是不方便的，并且序列号检查对于序列号的管理和销售是不方便的。

由 Ryouich Mori 提出的“超级销售”（super distribution）的概念指在保护软件所有者（以后称为信息提供者）的权利。这一概念在日本专利申请公开 Nos. 60－77218，60－191322，64－68835，2－4447，4－64129 等文件中实施了。图 1 说明了在日本专利申请公开 No.4－64129 中披露的“超级销售”的概念。信息提供者 P 向用户终端站 10 提供其所有的软件 ppi（或 ppj）。用户终端站 10 包括识别或判别单元 11 和存储单元 12。识别单元 11 判断软件 PP 是否允许使用，这借助于将软件识别数 PIDi（或 PIDj）和用户 ID/条件进行比较来实现。如果是可以使用的，则在存储单元 12 中存储所提供信息的使用历史。信息提供者 P 按照使用历史收取所提供的信息（软件 PP）的费用。标号“13”表示包括上述单元的软件服务单元（SSU）。

然而，“超级销售”系统和下述问题有关。

（1）在“超级销售”系统中，用户是否是信息提供者的订户由用

户的专用数据例如用户 ID 来判断。因此，需要配备至少一存储单元用以存储用户的专用数据。每个用户必须首先请求信息提供者以便接收使用许可和用户 ID 等，然后把用户 ID 或其类似物作为用户专用数据存储起来。这种订户许可程序是麻烦的并且大量用户的专用数据的管理要进行大量的工作。

（2）在“超级销售”系统中，用来存储软件使用历史的存储单元 12 被用来防止信息的非法使用并用来管理信息提供者提供的信息的使用状态。按照使用历史，信息提供者要求用户付费。在“超级销售”系统中，信息不被出售而是被租借，因而使使用历史成为必须的。然而，利用这种系统，信息提供者知道提供给用户的信息因而不能保护用户的私人密秘。

（3）利用“超级销售”系统，虽然被提供的信息的使用状态和费用可以正确地进行管理，但是没有披露费用支付装置及其方法。因此，在信息提供者检查被提供的信息的使用状态之后，提供者需要借助于使用另一系统请求收费并接收费用。

发明内容

本发明的目的在于解决上述问题（1）至（3）。

本发明的另一目的在于提供一种新的装置和系统，用来接收来自信息提供者的用于交易（counter value）的信息，这种装置或系统可以保护信息提供者的权利，并且使用方便，而且能为用户保密。

按照实现上述目的的本发明的一个方面，提供了一种费用计算装置，该装置包括：输入装置，用于输入表示金钱的金额的金额信息；允许信号输出装置，用于判断输入的金额信息和通过网络由提供者终端提供的电子信息的使用费用，以及根据该判断，输出允许信号以允许电子信息的使用；信息处理装置，用于在所述输出装置输出允许信号的情况下、执行处理以使得能够得到所述电子信息，在所述输出装置不输出允许信号的情况下，不执行所述处理；以及输出装置，用于输出执行了所述处理的电子信息。

按照本发明的另一方面，提供了一种费用计算方法，该方法包括：输入步骤，用于输入表示金钱的金额的金额信息；允许信号输出步骤，用于判断输入的金额信息和通过网络由提供者终端提供的电子信息的使用费用，以及根据该判断，输出允许信号以允许电子信息的使用；信息处理步骤，用于在所述输出装置输出允许信号的情况下、执行处理以使得能够得到所述电子信息，在所述输出装置不输出允许信号的情况下，不执行所述处理；以及输出步骤，用于输出执行了所述处理的电子

信息。

按照本发明的另一个方面，提供了一种信息提供系统，包括：提供者终端，用于提供电子信息；用户终端，用于使用通过网络从所述提供者终端接收的所述电子信息；收费装置，用于输入表示金钱金额的金额信息；判断装置，用于判断在所述收费装置输入的金额信息和所述电子信息的使用费用，以及根据该判断，输出允许信号以允许电子信息的使用；信息处理装置，用于在所述判断装置输出允许信号的情况下、执行处理以使得能够得到所述电子信息，在所述判断装置不输出允许信号的情况下，不执行所述处理；以及输出装置，用于输出执行了所述处理的电子信息。

本发明的上述的和其它目的当结合附图阅读以下对实施例的详细说明之后会更加清楚。

附图说明

图 1 是说明常规的超级销售系统的方块图。

图 2 是按照本发明第一实施例的收费装置和信息接收装置的方块图。

图 3 是按照本发明第二实施例的收费装置和信息接收装置的方块图。

图 4 是按照本发明第三实施例的收费装置和信息接收装置的方块图。

图 5 是具有第三实施例的收费装置和信息接收装置的通信系统的方块图。

图 6 是按照本发明第四实施例的收费装置和信息接收装置的方块图。

图 7 是具有第四实施例的收费装置和信息接收装置的通信系统的方块图。

图 8 是按照本发明第五实施例的收费装置和信息接收装置的方块图。

图 9 是按照本发明第六实施例的收费装置和信息接收装置的方块图。

图 10 是具有第六实施例的收费装置和信息接收装置的通信系统的方块图。

具体实施方式

现在参照图 2 到 10 说明本发明的实施例。

本发明的第一实施例参照图 2 进行说明。

在图 2 中，标号 10 代表作为信息接收装置的用户终端站，P 代表信息提供者，ppi（或 ppj）代表由信息提供者 P 提供的用于交易的信息，PIDi（或 PIDj）代表附加于 PPI 的专用数据，PPC 代表下文将要说明的钱的信息例如现金或信用卡，标号 14 代表 PPC 输入单元 ，标号 15 代表显示单元，标号 16 代表费用计算单元，其中包括 PPC 输入单元 14，显示单元 15 和识别或判断单元 16，用来判断所提供的信息 PP 是

否允许使用，标号17代表信号处理单元。

下面对其操作进行说明。

信息提供者P提供包括PID的信息PP。用户终端站10的结构使得当所提供的信息PP被使用时费用计算单元16总是被使用。费用计算单元16具有输入单元14，用来接收钱信息PPC。当使用所提供的信息PP的事件发生时，识别单元11按照PID与/或PPC检查被提供的信息PP的使用允许情况。例如，检查包含在PID中的使用费是否等于或小于由钱信息PPC表示的余额。允许（OK）或拒绝（NG）信号被送到信号处理单元17，如果允许，信号处理单元17则如此操作，使得用户可以使用所提供的信息PP。在PID与PPC上的信息(所提供信息的使用费、PPC的余额及其类似信息）在显示单元15上显示。由识别单元11产生的使用判断结果可以在显示单元15上显示。

在本发明中，钱信息PPC可以是现金、预付卡例如电话卡，存储在软盘内的电子的钱信息，IC卡或PCMCIA卡。在本发明中，代替利用用户专用的用户ID，利用不为用户所专用的钱信息PPC，来判断所提供的信息PP是否允许使用。因此，不要求用户提供用户ID，只需给出钱信息PPC，即只要支付所提供信息的使用费。这种处理是自然的而且容易的。因此，不需要管理大量的用户专用信息，所以可以解决问题（1）。

在本发明中，因为不给出用户专用数据，所以使用所提供的信息的秘密可以不提供给信息提供者。这表面看来似乎不保护信息提供者的权利，然而，只要付给信息提供者P相应于使用发生频率的费用就足够了，而不需要向信息提供者P提供使用所提供信息的秘密。虽然本发明不用使用历史存储单元存储由具有ID的用户使用的相应的PID的信息，但本发明可以具有使用发生频率存储单元用来存储哪个信息被使用了多少次的信息，并具有使用通知单元用来通知所提供的信息的当前使用情况。在图2中，通过由虚线所示的路径把使用发生频率通知信息提供者P。使用发生频率单元和使用通知单元的细节将在第二到第六实施例中给出。因此，用户保密的问题（2）可以得到解决。

在本实施例中，PPC是钱的信息并可通过使用PPC付费，从而可

以解决问题（3）。关于如何获得PPC如何收集PPC以及如何把钱分配给每个信息提供者的具体例子将在第二到第六实施例中和问题（2）一起进行说明。

费用计算单元16构成本发明的费用计算装置。虽然费用计算单元16被作为一个整体提供在用户终端站10内，但它也可以和用户终端站10分开提供。在这种情况下，费用计算单元16首先接收附加于由信息提供者P提供的信息PP上的信息PID，并且响应表示由识别单元11根据PID和PPC判断的允许的信息，用户终端10被允许接收所提供的信息PP并进行信号处理。这一方案也可以应用于后面要说明的第二至第八实施例中。

现在参照图3说明第二实施例。

在图3所示的实施例中，PPC是现金。在这种情况下，输入单元14具有硬币或纸币入口。用户首先向输入单元14输入一定数量的钱。如果输入的钱超过由PID指示的费用，则识别单元11就允许使用所提供的信息PP。在另一种结构中，费用计算单元16在显示单元15上显示所提供信息的使用费用，并且用户向输入单元14输入相应的钱。按照输入的钱，识别单元11检查所提供的信息是否允许被使用。在另一个替换的结构中，如果费用由于使用时间而改变，则这一结果被显示，并输入附加的费用。输入的钱被存储在币箱18中，并被信息提供者或某些收集钱的其它实体收集。每种所提供的信息PP的使用发生频率由计数器19记录，并且在币箱18中收集的费用按照使用发生频率分配给每个信息提供者P。如果只有一种被提供的信息被使用，并且不需计算使用发生频率，则可以省略计数器19。

下面参照图4说明第三实施例。

在图4所示的第三实施例中，PPC是一种预付卡例如电话卡。用户把预付卡插入PPC输入单元14中。识别单元11判断在预付卡上记录的钱是否大于使用费，如果大于，则允许使用PP。在这个例子中，使用费被在显示单元15上显示。在此实施例中，识别单元11和PPC输入单元14如此构成，使得甚至在PP的使用费随时间而改变时，如果费用小于在预付卡中记录的钱数，则PP可以被继续使用。如果输入单元14如此

构成，使得允许插入另外的预付卡，则可在较长的时间内使用 PP。

这种预付卡可以从预付卡零售店中容易地买到，象在电话卡的情况下一样。预付卡的制造者是费用分配者 20。每个信息提供者向费用分配者 20 登记，并按照所提供的信息 PP 的使用发生频率接受费用。费用分配者 20 包括预付卡零售店。

按照使用发生频率分配费用是借助于通过通信设备 I/F21 向费用分配者 20 通知来自费用计算单元 16 的当前使用信息来实现的。这种使用通报仅仅当费用计算单元 16 改变在预付卡中记录的钱数时才发出。如果通过通信设备接收所提供的信息 PP，则可以共用这个通信设备 I/F21。在这种情况下，如图 5 所示，费用分配者 20 的终端、信息提供者 P 的终端以及用户的终端 10 连到网络 22 上。费用分配者 20 按照上述的通知向信息提供者 P 分配收取的费用。

如果不使用通信设备 I/F，则可以使用对每一种所提供的信息不同的预付卡。在这种情况下，识别单元 11 检查每个预付卡的类型，并判断所提供的信息是否可被允许使用。另外，费用计算单元 16 可以配备用来在预付卡中记录所提供的信息 PP 的使用情况的装置。在这种情况下，费用分配者 20 收集预付卡，并按照使用发生频率分配费用。为了促进预付卡的收集，可以装有下述的系统。即，如果通过由旧的预付卡换新的预付卡来购买新预付卡，则只付在新预付卡中记录的钱数，而如果不购买新的预付卡，则只付预付卡本身的费用。没有被收集的预付卡的使用费用可以按照由已经收集的预付卡使用的费用的比例进行分配。

图 6 表示第四实施例，其中 PPC 是软盘或电子的与/或磁的容易被重写的存储装置。使用第四实施例的网络系统如图 7 所示。

存储在 PPC 中的钱信息是由银行或其它金融实体证明的或只允许由包括零售店在内的费用分配者 20 附加钱信息的特定数据。用户据 PPC 插入输入单元 14 中。费用计算单元 16 从 PPC 中读取钱信息，如果读出的钱信息大于可能被显示的在 PID 中记录的费用，并且如果费用计算单元 16 可以要求从 PPC 中支付，则识别单元 11 允许使用 PP。在这种情况下，即使使用费用随时间而改变，只要所用费用小于在 PPC 中记录的钱信息，则可以继续使用所提供的信息。

因为钱信息是电子钱信息，所以费用分配者20可以按预定程序通过通信设备I/F输入或输出钱信息。和第一第二实施例不同，用户不向费用分配者20支付现金。由和用户订有合同的银行或其它金融实体（以后称为费用供应人）保证用户的支付。和第三实施例类似，通过通信设备I/F21把当前使用信息通知费用分配者20，以便按照使用发生频率分配费用。在这种情况下，使用费用可以通过使用电子钱信息PPC直接送给费用分配者20或信息提供者。

具体地说，电子钱信息的输入/输出可通过下面的通信程序实现，假定费用计算单元16具有后面将要说明的编码/确认装置和后面将要说明的用于由TA表示的时间标记的安全管理的装置。这些装置用来确认PPC，并防止在时间标记管理下PPC的非法复制或类似问题，因为PPC是一种容易被重写的（例如软盘）介质。

费用计算和费用处理按下述14的假定进行说明。即假定用户“A”、信息提供者“B”、费用分配者“C”和费用供应人“D”中的每一个具有能够标记（signature）的秘密密钥，并且通信合作人具有能够检查该标记的公开密钥，其中“A”的秘密密钥由“SA”表示，A的公开密钥由“PA”表示。现在假定“A”使用由“B”提供的信息Pi。由“X”使用密钥“Y”获得的处理结果由{X}^Y表示，并且用户的每个处理以及密钥和时间标记的每个处理的管理假定由费用计算单元16中提供的具有保证安全性的装置进行，或根据用户的记忆或记录进行。

钱信息输入处理

（1）“A”借助于附加“A”的登记信息（例如帐号和信用卡号）并用秘密密钥“SA”标记向“C”发出a元（钱的单位不限于元）钱信息的输入请求信息MA。

MA ={A，{A, iA, a, TA}^SA}

（2）“C”通过使用“A”的公开密钥检查MA的标记，并通过使用登记信息“iA”向“D”要求a元的支付。如果该支付被确认收到，则“C”对“A”发出如下信息MC，该信息对钱信息“a”的每元或对每一基本单位“C”（如果被提供的信息的费用以100元为单位则对

每 100 元）用“C”的秘密密钥“SC”标记。每元或每个基本单位被附加有不同的时间标记（time stamp）Tci。

MC =Σ{TA, {C, e, TCi}^sC}^pA

（3）“A”使用“pA”对每个 MC 译码并用相应于“sC”的“C”的公开密钥检查标记。如果检查表明该标记正确，则{（C,a,TCi）}^sC 被写在 PPC 中。

TA 和 TCi 代表时间标记。具有相同发送器的相同时间标记的信息被判断为非法请求。TA 和 TCi 可以不是时间标记，而可以是在随机数之间极少相符的序列号或随机数。

使用信息通知处理

（1）如果“A”想使用信息“Pi”，假定在“A”的 PPC 中的钱信息大于记录在 PIDi 中的费用，则费用计算单元 16 允许使用 Pi。

（2）在“A”终止 Pi 的使用之后或在使用期间，费用计算单元 16 则从钱信息 PPC 中消去请求的费用。

（3）此时，“A”向“C”发出下面的使用信息 MB，其中“b”是消去的使用费用：

MB ={A, B, {B, b,TB}^sA}

（4）“C”检查这一信息，如果正确，则付给“B”“b”元作为分配的钱。

在以上说明中，在“C”和每个用户之间使用公开密钥密码系统以便简化处理。显然，使用秘密密钥的秘密密钥密码系统也可被使用。每个信息的有效项可以由从一个时间标记经过的时间确定。在以上说明中，在每个信息中数据元素的顺序可以是不规则的，并且在某些情况下，用户 A, B,…的 ID 数以及时间标记并不总是必须的。上述的钱信息输入处理和使用信息通知处理只是说明性的，并且不使用对用户为特定的数据的电子钱信息进行的费用计算处理也落在本发明的范围之内。

如果没有提供通信设备 I/F，则用户就到包括零售店在内的费用分配者 20 那里，付给相应于在 PPC 中存储的钱信息的钱，借以获得钱信息。当用户到包括零售店在内的费用分配者 20 那里补填钱信息时，如同信息 MB 的情况一样，可通过采集由费用计算单元 16 记录的被提供的信

息 PP 的 PPC 中的使用记录，按照使用发生频率进行费用分配。如上所述，因为电子钱信息是只能由费用分配者 20 进行处理的特定数据，所以没有通信设备 I/F21 的用户一定得到包括零售店在内的费用分配者 20 那里去，以便改变 PPC 的内容。因此，使用记录可以被收集并可以按照使用发生频率分配费用。

图 8 表示第五实施例，其中 PPC 是一种电子卡例如 IC 卡和 PCMCIA 卡。使用第五实施例的网络的结构和图 7 所示的相同。存储在 PPC 中的钱信息是由银行或其它金融实体证明的或只允许包括零售店在内的费用分配者增添钱信息的特定数据。用户把 PPC 插入输入单元 14 中，由预定的处理（例如检查通行字）启动 PPC 。费用计算单元 16 从 PPC 中读出钱信息，如果读出的钱信息大于在 PID 中记录的可以被显示的费用，并且如果费用计算单元 16 可以请求从 PPC 中支付，则识别单元 11 就允许使用 PP 。在这种情况下，即使使用费用随时间而改变，只要这费用小于记录在 PPC 中的钱信息，就可以继续使用提供的信息 PP 。

因为钱信息是电子钱信息，所以费用分配者 20 可以通过通信设备 I/F21 按照预定的程序输入或输出钱信息。和第一第二实施例不同，用户不向费用分配者 20 支付现金。由银行或其它金融实体，即由和用户订有合同的费用供应人 23 来保证用户的支付。和第三实施例类似，通过通信设备 I/F21 把当前使用信息通知费用分配者 20 ，以便按照使用发生频率分配费用。在这种情况下，可以使用电子钱信息 PPC 把使用费直接发给费用分配者 20 或信息提供者 P 。

具体地说，电子钱信息的输入/输出可由以下的通信程序实现。这里假定，为了通信和处理的安全性，用电子卡作为 PPC 的用户可通过通行字被证实，并且对 PPC 的数据存储器的访问可由访问条件进行控制，并且密码系统可以进行后面将要说明的加密和确认操作。假定用于加密和确认的秘密密钥被写入访问控制的存储器区域中，并且只有满足访问条件的人（发行卡的人，费用分配者，以及类似的人）才能进行访问。还假定除去卡的发行人或费用分配者 20 之外，都不能改变下述的收费操作。

用户终端站 10 、信息提供者 P 的终端、费用分配者 20 的终端，以

及费用供应人23的终端被连到网络22上，如图7所示，用户由“A”表示，信息提供者由“B”表示，费用分配者由“C”表示，费用供应人由“D”表示。“C”具有用来对每个用户进行密码通信的秘密密钥（例如，“A”和“C”之间的秘密密钥“SA”，“B”和“C”之间的秘密密钥“SB”）和只为“C”所知的秘密密钥“SC”，并且用于标记（signature）的相应的检查密钥是公开的。现在考虑“A”使用由“B”提供的信息Pi。使用密钥“Y”对简明句子“X”加密的句子由{X}^Y 表示，并假定用户的每个处理在具有安全功能的 PPC 中进行。

钱信息输入处理

（1）“A”通过附加“A”对“D”的登记信息“iA”（例如帐号和信用卡号）向“C”发出输入请求信息MA作为a元（钱的单位不限于元）的钱信息。

MA ={A, {A, iA, a, TA}^sA}

（2）“C”通过使用共用的“SA”对MA的加密部分解密，并使用“iA”要求“D”支付“a”元。如果该支付被确认收到，则“C”通过使用标记密钥“SC”给钱信息“a”作标记，并向“A”发出如下信息：

MC ={TA, {C, a, TC}^sC}^sA

（3）“A”使用“sA”对MC解密，并用相应于“sC”的“C”的公开密钥PC检查标记。如果检查表明是正确的标记，则把“a”元的钱信息加于PPC。

TA和TCi代表时间标记。具有相同发送器的相同时间标记的信息被判断为非法请求。TA和TC可以不是时间标记而是在随机数之间极少相重的随机数或序列号。

使用信息通知处理

（1）如果“A”想使用信息Pi，如果在“A”的PPC中的钱信息大于在PIDi中记录的费用，费用计算单元16就允许使用Pi。

（2）在“A”终止Pi的使用之后或在使用期间，费用计算单元16从钱信息PPC中减去所需的费用并把结果写入PPC中。

（3）与此同时，“A”向“C”发出如下使用信息MB，其中“b”是被减掉的使用费用。

MB＝{A, {B,b, TB}^sA}

（4）“C”对这一信息进行解密，如果正确，就向“B”支付“b”元作为被分配的钱。

如果通过加密在“A”和“B”之间传递信息，则在钱信息输入处理和使用信息通知处理之间进行如下的处理。假定“C”也和信息提供者“B”共用秘密密钥。

信息使用处理

（1）“A”向“C”发出如下的信息MA'，请求产生对于“B”的语音密钥。

MA'＝{A, B, TA'}

（2）“C”产生语音密钥CK并向“A”发出如下信息MC'。

MC'＝{{TC', A, CK}^sB, TA', B,CK}^sA

（3）“A”使用“sA”解密，MC'并向“B”发出{TC',A,CK}^sB。

（4）“B”通过使用“sB”对收到的信息解密，并把用语音密CK加密的信息送给“A”。

（5）“A”使用语音密钥CK对加密的信息解密。

在以上的说明中，为了简化处理，在“C”和每个用户之间使用秘密密钥密码系统。显然，类似于第五实施例，也可使用公开密钥密码系统。每个信息的有效项可由从一时间标记经过的时间确定。在以上的说明中，在每一信息中的数据元素的顺序可以是不规则的，并且在某些情况下，用户A，B，…的ID数和时间标记并不总是必须的。以上的钱信息输入处理和使用信息通知处理只是说明性的，使用不使用对用户为特定的数据的电子钱信息的费用计算处理也落在本发明的范围内。

如果不提供通信设备I/F，则用户到包括零售店在内的费用分配者20处得到被写入PPC中的钱信息。当用户到包括零售店在内的费用公配者20处以得到钱信息时，可以通过收集由费用计算单元16记录的被提供信息PP的PPC中的使用记录，按照使用发生频率进行费用分配。如

上所述，因为电子钱信息是只能由费用分配者20处理的特定数据，没有通信设备I/F21的用户必须到包括零售店在内的费用分配者20那里，以便改变PPC的内容。因此，使用记录可以被收集，因而可按照使用发生频率分配费用。

图9表示第六实施例，其中和第五实施例类似，使用电子信息作为钱信息并且不需要费用分配者20。

用户终端站10，信息提供者P的终端，以及费用供应人23的终端被连接到网络22上，如图9所示。假定使用电子卡作为PPC的用户可通过通行字确认，并且对PPC的数据存储器的访问可通过访问条件控制，并假定密码系统可以进行加密和确认操作。还假定用来加密和确认操作的密钥被写在访问控制的存储作器区域中。假定下述的费用计算操作除去卡发行人之外不能改变。

用户由“A”表示，信息提供者由“B”表示，费用供应人由“D”表示。假定它们每个都具有能够标记的秘密密钥，并且通信合伙人知道能够检查标记的公开密钥（例如“A”的密钥“sA”和“A”的公共密钥“pA”）。现在考虑“A”使用由“B”提供的信息Pi。由“X”使用“Y”进行处理的处理结果用{X}^Y表示，并假定用户的每一处理在具有安全性功能的PPC中进行。

钱信息输入处理

（1）“A”通过附加“A”的登记信息“iA”（例如帐号和信用卡号）向“D”发出输入请求信息MA作为a元的钱信息（钱的单位不限于元）

MA ={A, {A, iA, a, TA}^sA}

（2）“D”使用“A”的公开密钥“sA”检查MA的标记，如果“iA”是正确的，并且“a”可以支付“a”元，则给予钱信息“a”一个标记，并向“A”发出如下信息。

MD ={TA, {D,a, TD}^sD}^sA

（3）“A”通过使用“PA”检查MD，并用相应于“SD”的“D”的公开密钥PD检查作的标记。如果检查表明标记正确，则把“a”元的钱信息加到PPC。

TA 和 TD 代表时间标记。具有相同发送器的相同时间标记的信息被判断为非法请求。TA 和 TD 可以不是时间标记，而是序列号或是在随机数之间极少相重的随机数。

使用信息通知处理

（1）如果“A”想使用信息 Pi，当在“A”的 PPC 中的钱信息大于在 PIDi 中记录的费用时，费用计算单元 16 则允许使用 Pi。

（2）在“A”终止使用 Pi 之后或在使用期间费用计算单元 16 从钱信息 PPC 中减去所需的费用，并把结果写入 PPC 中。

（3）与此同时，“A”向“B”发出如下的使用信息 MB，其中“b”是减去的使用费。

MB ={A, B, {B, b, TB}^sA}

（4）“B”检查标记，如果正确，则通过对“D”表明“A”的标记{B, b, TB}^sA 接收“b”元。

如果通过使用密码在“A”和“B”之间传递信息，虽然通过合伙人的公开密钥可直接进行保密通信，但如果信息量大，则可按下述方法使用秘密密钥进行保密通信。在下述的步骤（1）和（2）中，“A”和“B”可以互换。

信息使用处理

（1）“A”借助于用“B”的公开密钥“pB”加密发送和“B”公用的密钥 CK。

MA'={A,B,CK,TA'}^pB

（2）“B”使用“sB”对收到的信息解密。

（3）“B”使用秘密密钥 CK 向“A”发出加密的信息。

（4）“A”通过使用秘密密钥 CK 对按收到的信息解密。

在上述的说明中，为简单起见，在“D”和每个用户以及信息提供者 P 之间使用公开密钥密码系统。显然，也可以使用秘密密钥密码系统。每个信息的有效项由从一时间标记经过的时间确定。在上述说明中，在每个信息中数据元素的顺序也以不规则，并且在某些情况下，用户 A，B，…的 ID 数以及时间标记并不总是必需的。以上的钱信息输入处理以及使用信息通知处理仅仅是说明性的，并且用不用对用户而言为特定的

数据进行的电子钱信息费用处理也落在本发明的范围之内。

下面说明其它的实施例

第七实施例

使用现金的第二实施例的费用计算单元可以应用于具有一个或几个用户终端站的费用计算系统。这种费用计算系统可由信息提供者 P 或费用分配者 20 安装在人口集中的地方，例如公共电话室、娱乐中心。茶馆和图书馆。人们可通过支付现金接收信息。

使用预付卡的第三实施例的费用计算单元可以应用于这样的费用计算系统，其中信息提供者 P 通过 CD - ROM 、个人计算机通信设备等广泛地分发信息 PP，费用分配者 20 可以是某些制造和销售预付卡的版权团体，用户在零售店之类的地方购买预付卡，从而在家中或在其它的终端上接收提供的信息 PP 。

使用软盘的第四实施例的费用计算单元可以应用于这样的费用计算系统，其中例如被第三实施例使用的专用 PPC 输入单元 14 是不需要的，因为用户终端站通常配备有软盘输入单元 14，零售店也是不需要的，因为可以通过通信设备给出钱信息，并通过使用软件进行加密和确认操作。这种费用计算系统可借助于当前网络系统容易地实现。

使用电子卡例如 IC 卡和 PCMCIA 卡的第五实施例的费用计算单元可应用于这样的费用计算系统中，这种系统比使用第四实施例的费用计算系统具有更可靠的安全功能。

第六实施例的费用计算单元可以应用于这样的费用计算系统中，其中不需要费用分配者 20，而用户和信息提供者 P 通过费用供应人 23 直接联络。费用计算单元和费用计算系统显然可以应用于使用专用数据的电子钱，这在不久的将来即可付诸实用。

本发明的范围也包括费用计算单元和费用计算系统的组合。

第八实施例

在现在已知的费用计算系统中，信息提供者在 CD - ROM 中存储由不同密钥加密的几组信息。CD - ROM 本身在零售店以低价销售。如果用户需要某一信息，则信息提供者告诉那一信息的密钥并收取一定费用。不过，利用这种系统，零售店收取除去所提供的信息的费用之外的

CD－ROM销售利润的一部分。

这一问题可以通过使用本发明的PPC费用计算单元不是出租信息而是出售信息来解决。具体地说，用户购买CD－ROM和PPC例如预付卡。当通过通信设备（电话之类）由信息提供者告诉密码密钥时使用预付卡。信息提供者从零售店收到费用。用这种方式，零售店也可以从所提供的信息中获得一些利润。在这种情况下，费用计算单元16检查PPC钱信息，并且如果所提供的信息允许使用，当信息被解密时则从PPC中减去使用费。如果不使用PPC，钱可以退回。PPC由每个提供者制造并在零售店象CD－ROM一样出售。

在这一系统中，费用分配者不再需要。如果第三实施例的使用信息通知处理按下述方式修正，则对于预付卡的处理可以提供较高的安全性。不过要假定每个预付卡具有ID数“iP”和相应的秘密密钥“sP”。

使用信息通知处理

（1）如果在“A”的PPC中的钱信息大于在PIDi中记录的费用，则识别单元就允许使用信息Pi。

（2）在“A”终止Pi的使用之后或者在使用期间，识别单元从钱信息PPC中减去所需的费用，并把结果写入PPC中。

（3）与此同时，识别单元向“C”发出如下的使用信息MB，其中“b”是为“B”减去的使用费。

MB＝{iP, {B, b, iP,TB}^sP}

（4）“C”通过使用登记的秘密密钥“sP”对MS解密，如果正确，就向“B”支付“b”作为分配的费用。

按上述方式，除去知道“iP”和“sP”的人之外，不能发出使用信息。

下面说明秘密密钥密码系统和公开密钥密码系统。

秘密密钥密码系统（common key cryptosystem）是这样一种密码系统（也叫作秘密密钥密码系统（Secret key cryptosystem），对称密码系统（a Symmetry cryptosystem）以及公用使用密码系统（a Common use cryptosystem）），其中发送机和接收机共用同一密钥。公用密码系统可以分为块密码（block cipher）和流密码（stream

cipher ）两类，前者用同一密钥加密一个合适长度的字符串（块），后者用不同密钥加密每个字符串或位。块密码包括借助于置换字符顺序的置换密码加密和借助于改变字符为不同字符的字符改变密码加密。在这些情况下，用置换和字符改变的对应表作为加密密钥（ encipher key ）。

已知的流密码包括使用多个表的 Vigenere 密码和使用一次性处理密钥的 Vernam 密码（每个密码的详细内容请参见 Ikeno 和 Koyama 的“ Modern Cipher Theory ” IEICE， 1986，第二和第五段）。在块密码中， DES （ Data Encryption Standard ）和 FELA （ Fast Data Encipherment Algorithm ）被广泛地用作商业密码，因为它们的算法已经公开（详细情况请参见 Tsujii 和 KasAhara “ Cipher and information security ” ,shoukoudo, 1990,第二段）。

因为 DES 和 FELA 的算法已经公开，所以它们被以各种形式进行修正，以便防止解密。例如，下文将要说明的重复数被增加（参见 C. H.Mayer 和 S. M. Matyas “ CRYPTOGRAPHY － A New Dimension in Compnter Data Security ”, Willey － Interscience, Appendix D, PP.679 to 712, 1982 ）以及密钥被频繁地改变（参见 Yamanoto, Iwamura, Matsumoto, 和 Imai “ Squara Type Quasi Random Number Generator and Practical Ciphering with Block Cipher ”, Technical Report, IEICE, ISEC93-29, PP.65 至 75， 1993 ）。

公开密钥密码系统（ Public key cryptosystem ）

在公开密钥加密系统中，加密密钥和解密密钥是不同的，前者是公开的，而后者被保持为密秘的。其特点（ a ），协议（ b ）和典型例子（ c ）如下：

（ a ）公开密钥密码的特点

（ 1 ）因为加密密钥和解密密钥是不同的，并且加密密钥是公开的，所以不需要秘密地发送加密密钥因而有利于发送。

（ 2 ）每个用户的加密密钥是公开的，从而使每个用户只需保持其解密密钥为秘密状态。

（ 3 ）可以实现确认功能，这一功能使得接收机可以确认收到的通信文本不是伪造的或修改过的。

（b）公开密钥密码的协议

公开密钥算法满足下面两个条件，其中通信句子用M表示，用公开加密密钥“Kp”的加密用E（Kp,M）表示，用秘密解密密钥“KS”的解密用D（Ks,M）表示。

（1）当给定“Kp”时，E（Kp,M）的计算是容易的。当给定“KS”时，D（KS,M）的计算是容易的。

（2）如果“KS”未知，即使已知“Kp”、E的计算程序和C＝E（Kp,M），从计算量的观点来看确定M也是困难的。

除去条件（1）和（2）之外，如果下述的条件（3）满足，则可以实现秘密通信。

（3）对所有的通信文本（简明文本）M，可以确定E（Kp,M）和满足D（KS，E（Kp,M））＝M的条件。即，因为“Kp”是公开的，任何人可以计算E（Kp,M）。然而，只有具有秘密密钥“KS”的人才能通过计算D（KS，E（Kp,M））获得M。如果除条件（1）、（2）之外，还满足下述条件（4），则可以实现确认通信。

（4）对所有通信文本（简明文本）M，可以确定D（KS,M）以及满足E（Kp,D（ks',M））＝M的条件。即，只有具有秘密密钥“KS”的人才可以计算D（KS，M）。即使另一个人通过使用伪造的秘密密钥KS'计算D（KS'，M），接收机也可以证实该信息是伪造的，因为E（Kp,D（RS',M））和M不同。即使D（KS,M）是伪造的E（Kp,D（KS,M）'）也和M不同，因而接收机可以确认收到的信息是假的。

在公开密钥密码系统中，使用公开密钥的处理E叫作加密，使用秘密密钥的处理D叫作解密。对于秘密通信，发送机进行加密，接收机进行解密。对于确认通信，发送机进行解密，而接收机进行加密。

下面说明协议，其中在发送机“A”中使用公开密钥密码，并对于接收机“B”进行秘密通信、确认通信、具有标记的秘密通信。“A”的秘密密钥由“ksA”表示，“A”的公开密钥由“kpA”表示，而“B”的秘密密钥由“ksB”表示，“B”的公开密钥由“kpB”表示。

秘密通信

从“A”到“B”的通信文本（简明文本）的秘密通信使用下述程序进行。

步1：“A”使用“B”的公开密钥“kpB”加密M，并向“B”发出加密的文本C。

C = E（kpB,M）

步2：“B”使用“B”的秘密密钥“ksB”解密C，从而获得原来的简明文本M。

H = D（ksB,C）

因为接收机“B”的公开密钥是公开的，不限于“A”的任何人都可和“B”进行秘密通信。

确认通信

从“A”到“B”的通信文本（简明文本）的确认通信按下述程序进行。

步1：“A”使用“A”的秘密密钥“ksA”产生发送文本S，并把它发送给“B”。

S = D（ksA,M）

这一发送文本叫作标记文本，并把产生标记句子的操作叫作标记。

步2：“B”使用“A”的公开密钥“kpA”解密S，从而获得原来的简明文本。

M = E（kpA,S）

如果证明M是具有某些意义的文本，则确认M是已经从“A”发出的。

因为发送器“A”的公开密钥是公开的，所以不限于“B”任何人都可以确认“A”的标记文本。

这种确认也叫作数字标记。

具有标记的确认通信

从“A”到“B”的具有通信文本（简明文本）的标记的确认通信按下述程序进行。

步1：“A”使用“A”的秘密密钥“ksA”通过S的标记产生标记文本S。

S = D（kpA,M）

“A”使用“B”的公开密钥进一步加密S，并向“B”发送加密的文本C。

C = E（kpB,S）

步2：“B”使用“B”的秘密密钥“ksB”解密C，从而获得标记文本S。

S = D（ksB,C）

“B”使用“A”的公开密钥“kpA”进一步解密S，从而获得原来的简明文本M。

M = E（kpA,S）

如果证明M是具有某些意义的文本，则确认M是从“A”发出的。

在具有标记的秘密通信的每步的函数顺序可以颠倒。具体地说，步1：C = E（kpB,D（ksA,M））以及步2：M = E（kpA,D（ksB,C））可以颠倒为步1：C = D（ksA,E（kpB,M））和步2：M = D（ksB,E（kpA,C））。

（C）典型的公开密钥密码系统

公开密钥密码系统的典型例子列举如下。

能够进行秘密通信和确认通信的密码系统列举如下。

RSA密码系统：R.L.Rivest, A. Shamir和I。Adlcman“取得数字签名和公共密钥密码系统的方法”，Comm. Of ACM, 1978.

R密码系统：M.Rabin“数字签名及公共密钥密码系统”，MIT/LCS/TR-212, Technical Report MIT.1979.

W密码系统：H.C.Williang“RSA公共密钥加密过程的改良”，IEEE Trans. Inf. Teory, IT-26, 6, 1980。

MI密码系统：T.Matsumoto和H.Imai“公共密钥密码系统的新算法”，Technical Report, IT-82-84;1982, IEICE;和T.Matsumoto以及H.Imai“一类基于有限环上多项式的非对称密码系统”，信息理论的IEEE International Symp., 1983。

只能够进行秘密通信的密码系统列举如下：

MH密码系统：R.C.Merkle和M.E.Hellman“隐含信息及陷入渐

缩签名”, IEEE Trans. Inf. Theory, IT-24, 5, 1978 。

GS 密码系统: A.Shamir 和 R.E.Zippel “关于 Morkle – Hellman 密码法的安全”, IEEE Trans. Inf. Theory, IT-26, 3, 1980 。

CR 密码系统: B. Chor 和 R.L.Rivest 。

“基于算术无穷域的背包式公共密钥密码系统”, Proc. Crypto. 84 。

M 密码系统: R.J.Mcelioce “基于代数编码理论的公共密钥密码系统”, PSN Progress Rep. Jet Propulsion Lab. 1978 。

E 密码系统: T.E.Eicamal “基于离散算法的公共密钥密码系统和签名法”, Proc. Crypto. 84, 1984 。

T 密码系统: Shigeo Tsujii “使用矩阵因子分解的公共密钥密码系统”, Technical Report, IEICE, IT8512, 1985 。

只能够进行确认通信的密码系统列举如下。

S 密码系统: A.Shamir “快签名法”, report MIT/LCS/TM-107,Mil 计算机科学实验室 Cambridge, Mass.1978 。

L 密码系统: K. Leiberherr “一致复杂度及数字签名”,计算机科学 115 自动化语言及编程中的讲义,Eighth Colloguium Acre, Israel, 1981 。

GMY 密码系统: S.Goldwasser, S.Micali 和 A.Yao “强签名法 ”, 计算理论的 ACM Symp.,1983 。

GMR 密码系统: S.Goldwasser, S.Micali 和 R.L.Rivest “签名问题的真正解决”, ACM Symp. 关于计算机科学的基础, 1984 。

OSS 密码系统: H.Ong, C.P.Schnorr 和 A.Shamir “基于二次式的有效签名法”,ACM Symp.关于计算理论, 1984 。

OS 密码系统: T.Okamoto 和 A.Shiraishi “基于多项式计算的数字签名法”, IEICE,(D), J86-D,5, 1985,以及 T. Okamoto 和 A.Shiraishi “基于二次不等式的快签名法”, IEEE Symp. 关于计算理论, 1984 。

如上所述, 按照本发明, 可以实现解决上述的多媒体网络的问题(1)到(3)的费用计算装置和费用计算系统。

每个用户可以用低的费用租借各种信息同时又能保密。信息提供者

可以按照所提供的信息的使用发生频率收取费用，而不用信息提供者对每个用户对所提供的信息的使用进行管理。通过结合包括零售店在内的费用分配者和费用供应人，可以构成容易使用的具有费用支付功能的费用计算系统。

本发明的许多不同的实施例可以被构成而不脱离本发明的范围。应当理解本发明并不限于说明书中描述的具体实施例，而是由所附权利要求进行限定。

图 1

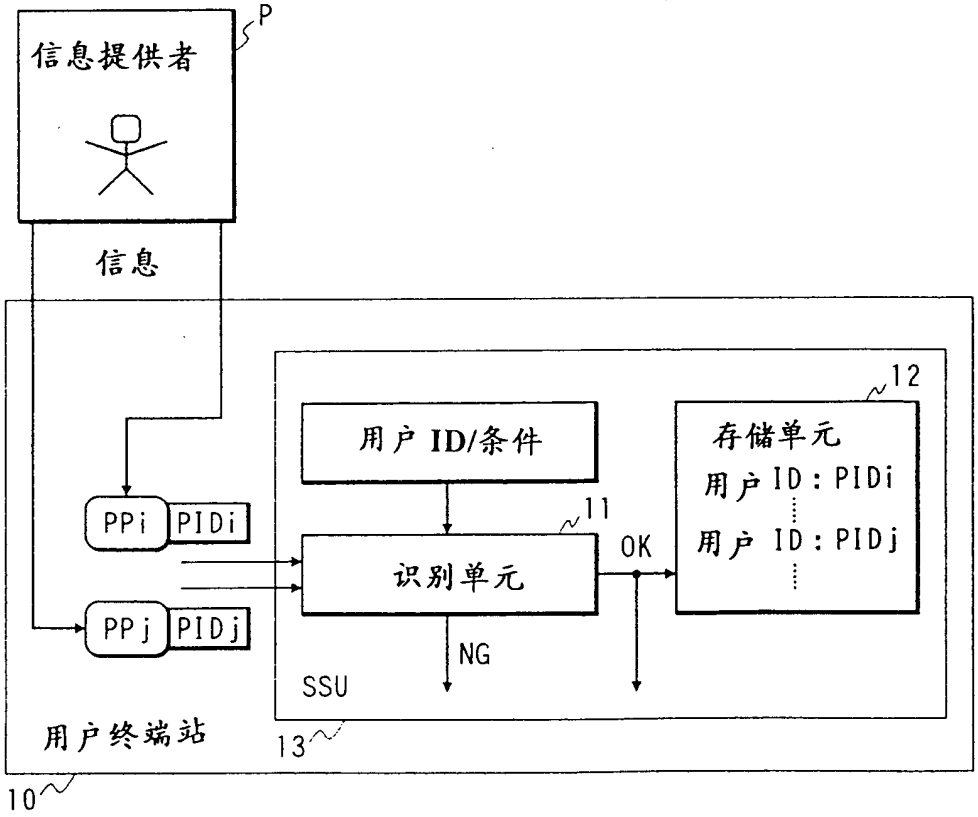

信息提供者
P
信息
PPi
PIDi
PPj
PIDj
用户终端站
10
用户 ID/条件
11
识别单元
OK
NG
SSU
12
存储单元
用户 ID：PIDi
用户 ID：PIDj
13

图 2

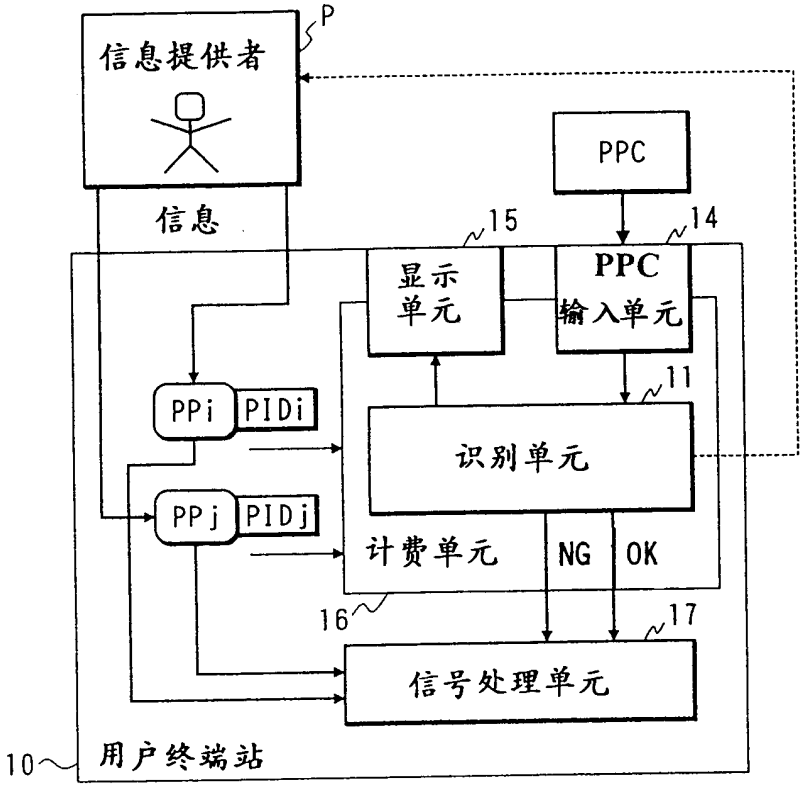

信息提供者
P
PPC
信息
15
14
显示
单元
PPC
输入单元
11
PPi
PIDi
识别单元
PPj
PIDj
计费单元
NG
OK
16
17
信号处理单元
10
用户终端站

图 3

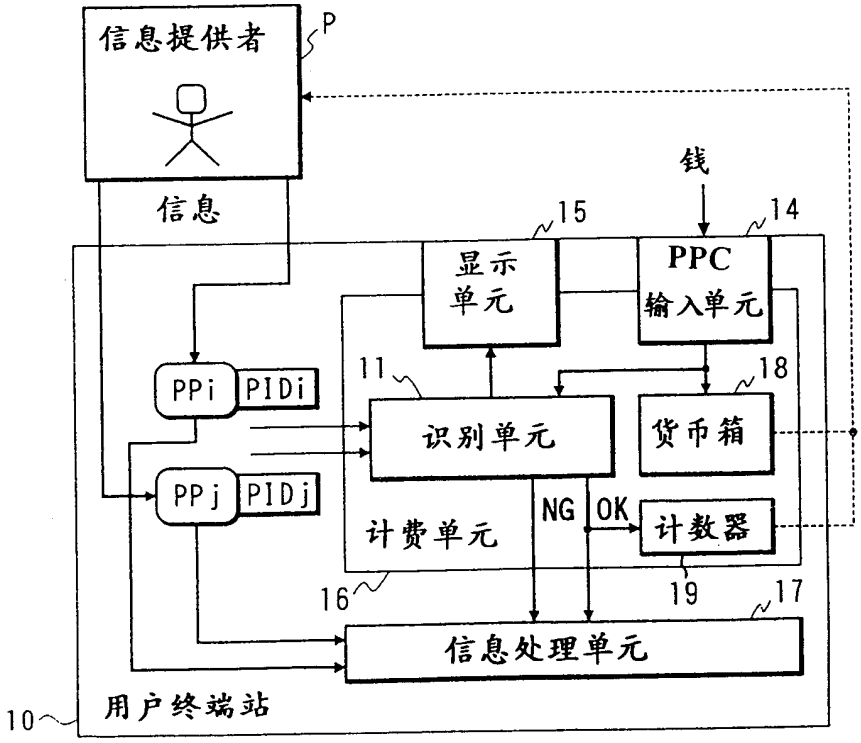

信息提供者
P
钱
信息
15
14
显示
单元
PPC
输入单元
11
18
PPi
PIDi
识别单元
货币箱
PPj
PIDj
计费单元
NG
OK
计数器
16
19
17
信息处理单元
10
用户终端站

图 4

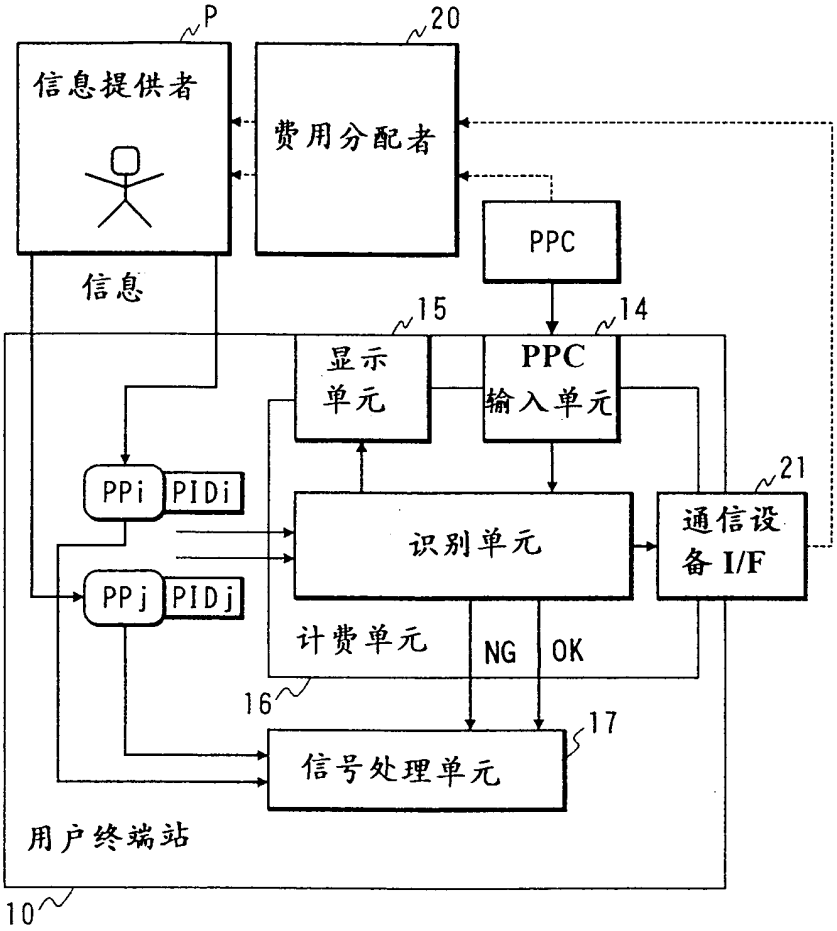

P
20
信息提供者
费用分配者
PPC
信息
15
14
显示
单元
PPC
输入单元
21
PPi
PIDi
识别单元
通信设
备 I/F
PPj
PIDj
计费单元
NG
OK
16
17
信号处理单元
用户终端站
10

图 5

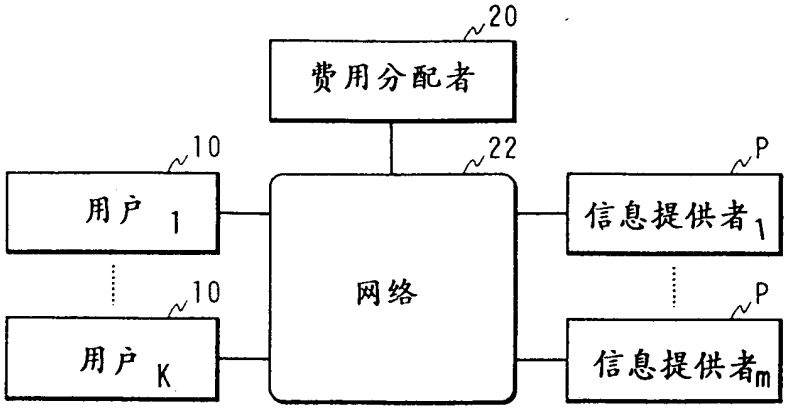

20
费用分配者
10
22
P
用户 1
信息提供者1
网络
10
P
用户 K
信息提供者m

图 6

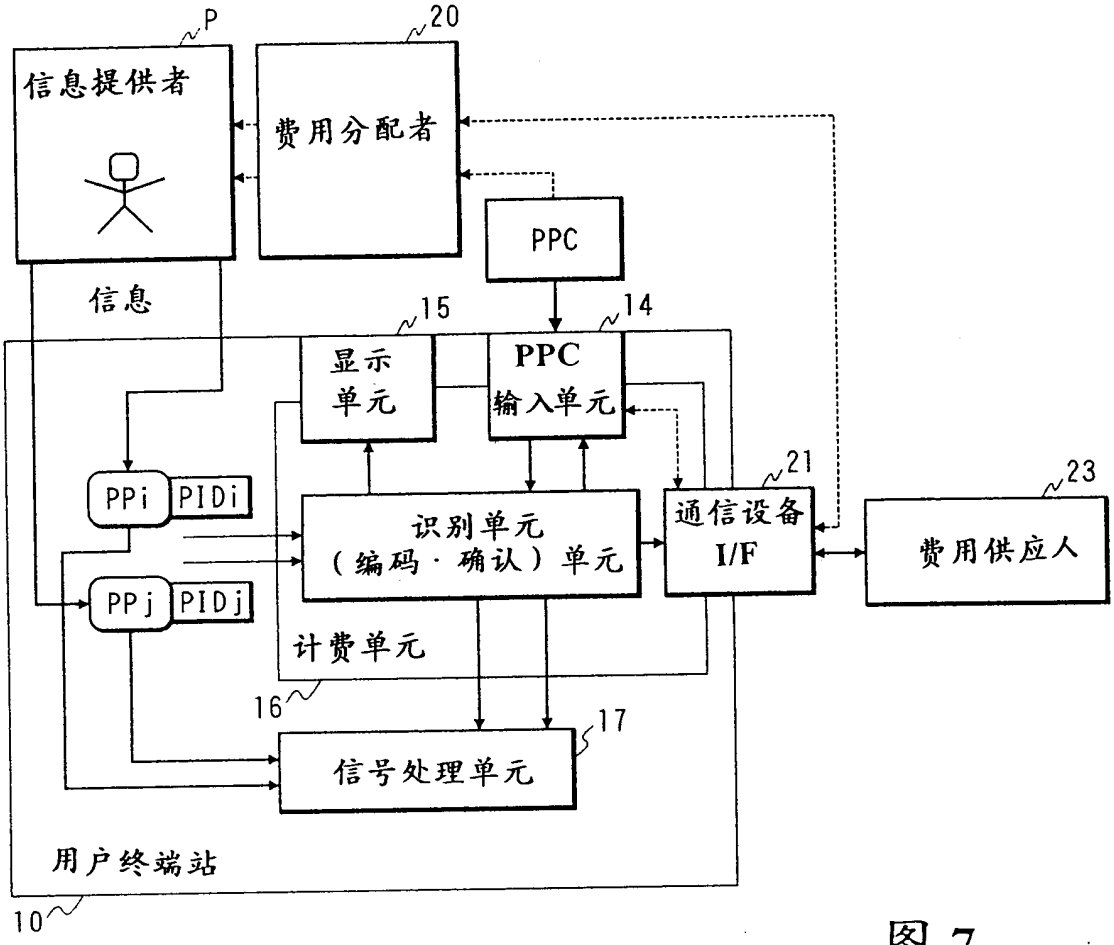

P
20
信息提供者
费用分配者
PPC
信息
15
14
显示
单元
PPC
输入单元
21
23
PPi
PIDi
识别单元
（编码·确认）单元
通信设备
I/F
费用供应人
PPj
PIDj
计费单元
16
17
信号处理单元
用户终端站
10

图 7

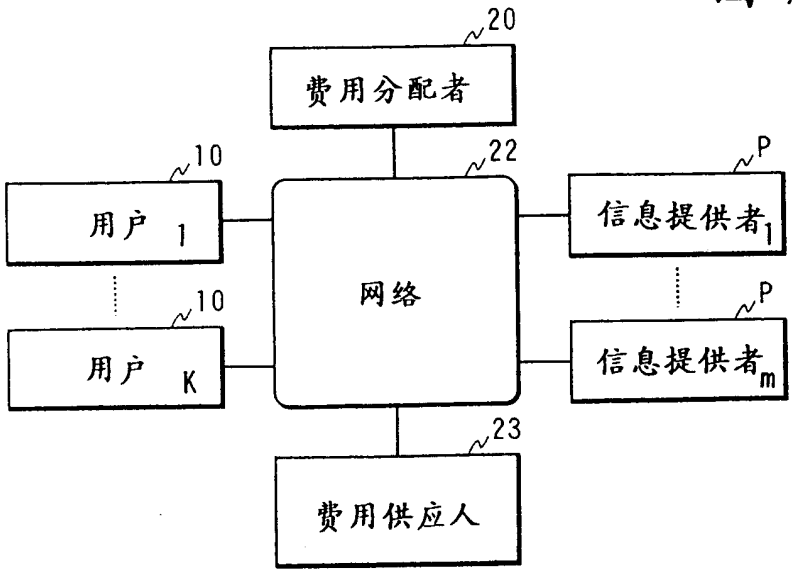

20
费用分配者
10
22
P
用户 1
网络
信息提供者1
10
P
用户 K
信息提供者m
23
费用供应人

图 8

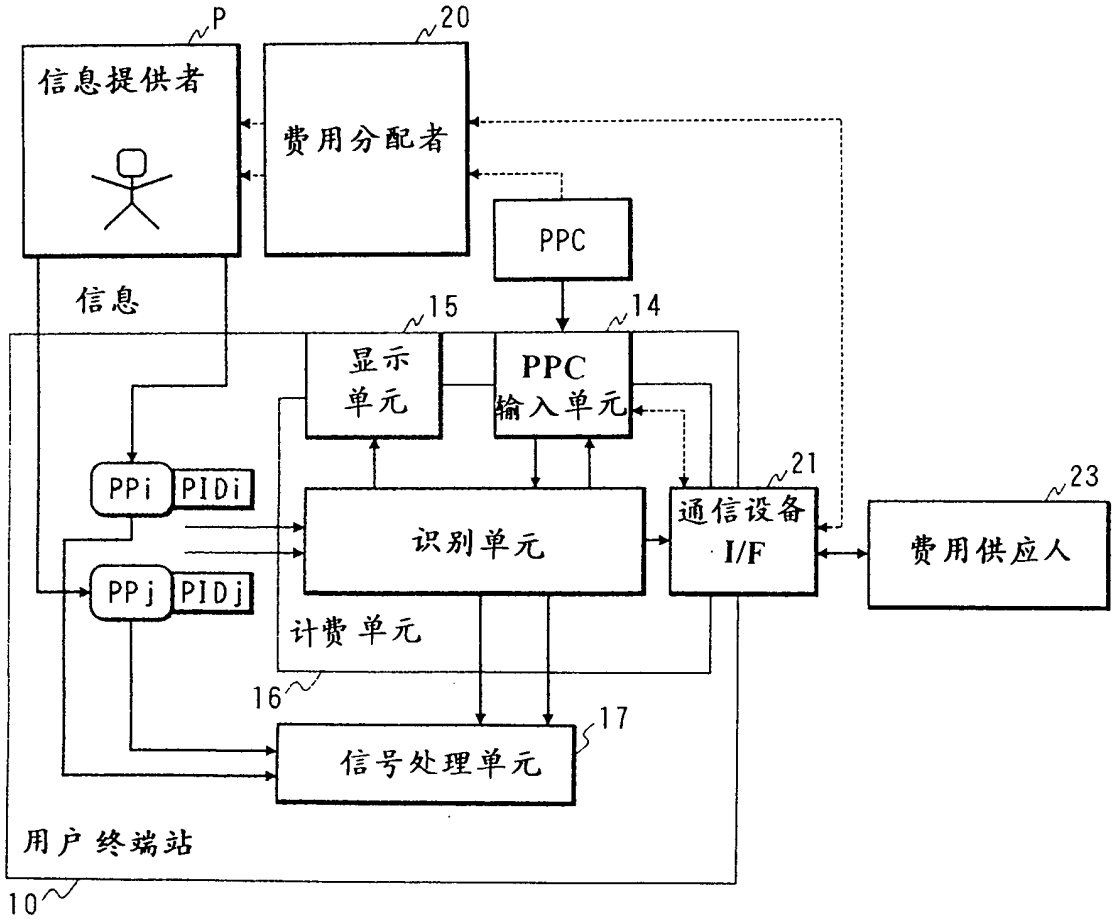

P
20
信息提供者
费用分配者
PPC
信息
15
14
显示
单元
PPC
输入单元
21
23
PPi
PIDi
识别单元
通信设备
I/F
费用供应人
PPj
PIDj
计费单元
16
17
信号处理单元
用户终端站
10

图 9

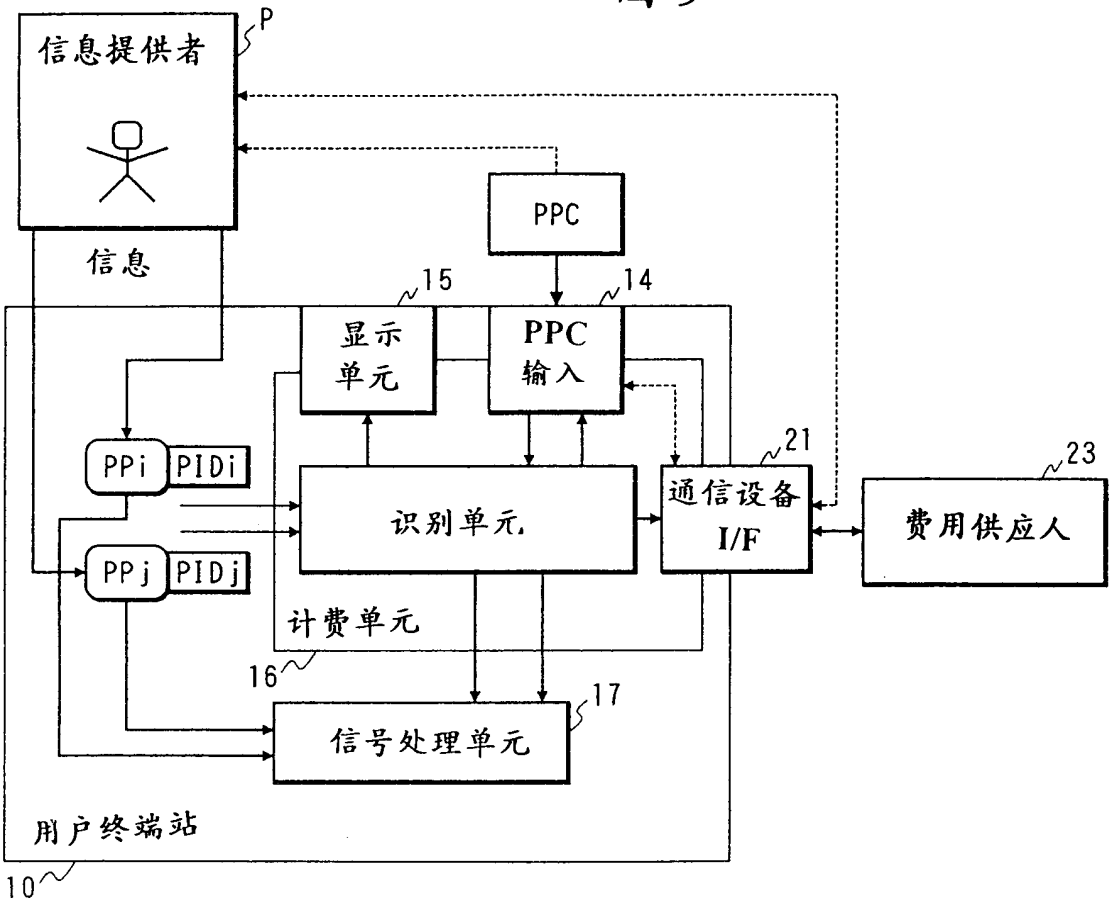
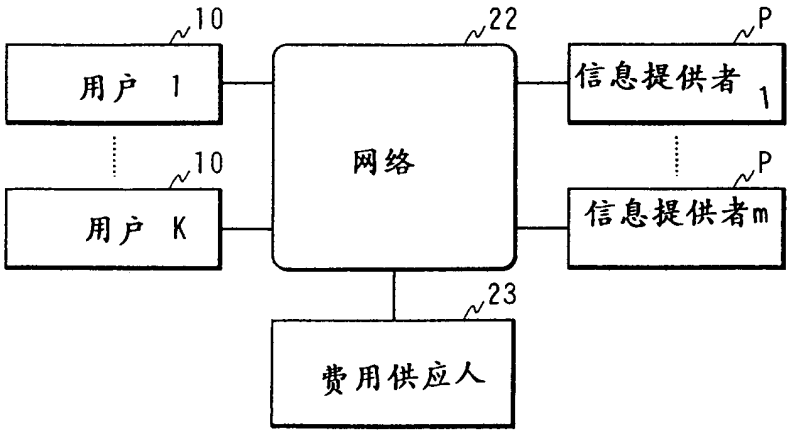

信息提供者
P
信息
PPC
15
显示
单元
14
PPC
输入
21
通信设备
I/F
23
费用供应人
PPi
PIDi
PPj
PIDj
识别单元
计费单元
16
17
信号处理单元
用户终端站
10

图 10


10
用户 1
10
用户 K
22
网络
P
信息提供者 1
P
信息提供者m
23
费用供应人