(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1798021 B
(45)授权公告日 2011.09.14

(21)申请号 200510097519.7

(22)申请日 2005.12.28

(30)优先权数据
2004-379775 2004.12.28 JP

(73)专利权人 株式会社日立制作所
地址 日本东京都

(72)发明人 高田治 藤城孝宏 锻忠司 星野和义

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 郝庆芬

(51)Int.Cl.
H04L 9/00(2006.01)

(56)对比文件
JP 2003-101533 A,2003.04.04, 全文.
JP 2004-159100 A,2004.06.03, 全文.
JP 2004-80512 A,2004.03.11, 全文.
JP 2004-56628 A,2004.02.19, 全文.

审查员 郭风顺

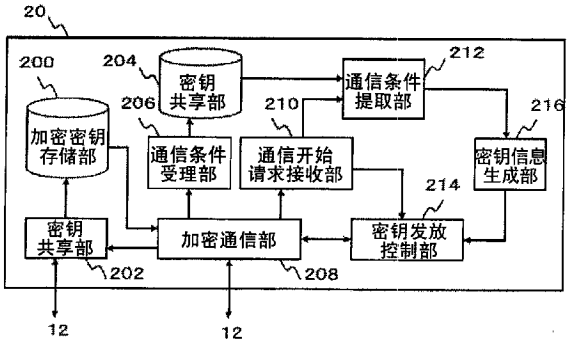
权利要求书 4 页 说明书 15 页 附图 8 页

(54)发明名称

通信支持服务器、通信支持方法、及通信支持系统

(57)摘要

提供一种通信支持服务器(20),它能减少伴随开始通信的信息处理装置(14)的认证处理产生的处理负荷。通信支持服务器(20)的加密通信部(208),当在与信息处理装置(14)间收发信息时,在与该信息装置(14)的识别信息对应起来存储在加密密钥存储部(200)的第一密钥的有效期在经过之前时,就省略认证信息处理装置(14)的处理,用该第一密钥在与该信息处理装置(14)间进行加密通信,在该有效期经过之后时,或与该信息处理装置(14)的识别信息对应的第一密钥没有存储在加密密钥存储部(200)时,就让密钥共享部(202),进行认证处理和用于与该信息处理装置(14)间的加密通信的第一密钥的共享处理,并用新共享的第一密钥进行与该信息处理装置(14)的加密通信。



CN 1798021 B

1. 一种通信支持服务器，其特征在于，

该通信支持服务器，支持通信终端之间的加密通信，

具有：

通信条件存储部，其对于每个所述通信终端，将该通信终端可实施加密通信的通信条件，与该通信终端的识别信息对应起来进行存储；

密钥共享部，其在与所述通信终端之间，进行作为用于与该通信终端间的加密通信的密钥的第一密钥的共享；

第一密钥存储部，其将通过所述密钥共享部在与所述通信终端之间共享的第一密钥，与对应的有效期限一起，与所述终端的识别信息对应起来进行存储；

加密通信部，其采用所述第一密钥，与具有与该第一密钥对应的识别信息的通信终端进行加密通信；

共通通信条件提取部，其采用经由所述加密通信部从所述通信终端接收到的通信开始请求内所包含的 2 个所述通信终端的识别信息并参照所述通信条件存储部，将作为该 2 个通信终端共通的通信条件的共通通信条件提取出来；和

第二密钥信息生成部，其生成遵从所提取出的共通通信条件的第二密钥信息，并将已生成的第二密钥信息与所述共通通信条件一起，经由所述加密通信部发送到所述 2 个通信终端的每一个；

所述加密通信部，当向所述通信终端请求加密通信时，

当是与该通信终端的识别信息对应的第一密钥的有效期限的经过之前时，就采用与该通信终端的识别信息对应起来存储在所述第一密钥存储部的所述第一密钥，向该通信终端请求加密通信，

当是所述第一密钥的有效期经过之后时，或当与该通信终端的识别信息对应的第一密钥没有存储在所述第一密钥存储部时，就让所述密钥共享部，进行所述第一密钥的共享，并采用新共享的第一密钥向该通信终端请求加密通信。

2. 如权利要求 1 所述的通信支持服务器，其特征在于，

还配备从所述通信终端，经由所述加密通信部，受理该通信终端的识别信息及通信条件，并存储在所述通信条件存储部的通信条件受理部。

3. 如权利要求 1 所述的通信支持服务器，其特征在于，

还配备密钥发放控制部，该密钥发放控制部，当经由所述加密通信部，从进行通信的所述 2 个通信终端的一方接收到所述通信开始请求时，将所述第二密钥信息生成部生成的第二密钥信息，与该通信开始请求一起向所述 2 个通信终端的另一方发送，并应答所发送的通信开始请求，当经由所述加密通信部从所述另一方接收到通信开始许可时，将所述第二密钥生成部生成的第二密钥的信息，与接收到的通信开始许可一起向所述一方发送。

4. 如权利要求 1 所述的通信支持服务器，其特征在于，

还配备第一密钥删除部，该第一密钥删除部，参照所述第一密钥存储部存储的各个的第一密钥的有效期限，将现在的时间超过了所述有效期限的第一密钥从所述第一密钥存储部删除。

5. 如权利要求 4 所述的通信支持服务器，其特征在于，

还配备密钥发放控制部，该密钥发放控制部，当经由所述加密通信部，从进行加密通信

的所述 2 个通信终端的一方接收到所述通信开始请求时，将所述第二密钥信息生成部生成的第二密钥信息，与该通信开始请求一起向所述 2 个通信终端的另一方发送，应答已发送的通信开始请求，当经由所述加密通信部从所述另一方接收到通信开始许可时，将所述第二密钥生成部生成的第二密钥的信息，与接收到的通信开始许可一起向所述一方发送。

6. 如权利要求 4 所述的通信支持服务器，其特征在于，

还配备通信条件受理部，该通信条件受理部，从所述通信终端，经由所述加密通信部，受理该通信终端的识别信息及通信条件，并存储在所述通信条件存储部。

7. 如权利要求 6 所述的通信支持服务器，其特征在于，

还配备密钥发放控制部，该密钥发放控制部，当经由所述加密通信部，从进行通信的所述 2 个通信终端的一方接收到所述通信开始请求时，将所述第二密钥信息生成部生成的第二密钥信息，与该通信开始请求一起向所述 2 个通信终端的另一方发送，应答已发送的通信开始请求，当经由所述加密通信部从所述另一方接收到通信开始许可时，将所述第二密钥生成部生成的第二密钥的信息，与接收的通信开始许可一起向所述一方发送。

8. 一种通信支持方法，其特征在于，

该方法，是通信支持服务器支持通信终端之间的加密通信的通信支持方法，

所述通信支持服务器，

具有：

通信条件存储部，其在所述每个通信终端，将该通信终端可实施加密通信的通信条件，与该通信终端的识别信息对应起来进行存储；和

第一密钥存储部，其在所述每个通信终端，将作为用于与该通信终端间的加密通信的密钥的第一密钥，与对应的有效期限一起，与所述通信终端的识别信息对应起来进行存储；

所述通信支持方法，

具有：

通信开始请求取得步骤，其把从所述终端接收到的已被加密的通信开始请求，用与该通信终端的识别信息对应起来存储在所述第一密钥存储部的所述第一密钥进行解密后，取得包含开始通信的 2 个所述通信终端的识别信息的通信开始请求：

共通通信条件提取步骤，其用所取得的所述通信开始请求内包含的 2 个所述通信终端的识别信息，参照所述通信条件存储部，提取作为该 2 个通信终端共通的通信条件的共通通信条件；

第二密钥信息生成步骤，其生成依照提取出来的共通通信条件的第二密钥信息；

第二密钥信息发送步骤，其对于包含于所述通信开始请求内的 2 个通信终端的每一个，采用与该通信终端的识别信息对应的第一密钥，将所述提取出来的共通通信条件及所述已生成的第二密钥信息加密后进行发送；和

密钥共享步骤，其在所述通信开始请求取得步骤及所述第二密钥信息发送步骤的每一个之前，如果是所述第一密钥的有效期限经过之后时，或对应 该通信终端识别信息的所述第一密钥没有存储在所述第一密钥存储部时，进行所述第一密钥的共享，将新共享的第一密钥，与该第一密钥的有效期限一起，与该通信终端的识别信息对应起来存储到所述第一密钥存储部。

9. 一种通信支持系统，其特征在于，

该通信支持系统，支持通信终端之间的加密通信，

具有：

多个所述通信终端；和

支持所述通信终端之间的通信的通信支持服务器；

所述多个终端的每一个，

具有：

终端侧密钥共享部，其进行作为用于所述通信支持服务器之间的加密通信的密钥的第一密钥的共享；

终端侧第 1 密钥存储部，其将所述第一密钥，与所述第一密钥的有效期限对应起来进行存储；

终端侧加密通信部，其用所述第一密钥，在与所述通信支持服务器之间进行加密通信；

通信开始请求发送部，其将自身及通信对方的所述通信终端的识别信息，经由所述终端－服务器间加密通信部，与通信开始请求一起发送给所述通信支持服务器；

第二密钥信息接收部，其响应所述通信开始请求发送部与所述识别信息一起已发送的通信开始请求，接收作为用于在所述自身以及在通信对方的通信终端之间的加密通信的密钥的或用来算出该密钥的种信息的第二密钥信息；

第二密钥存储部，其将所述第二密钥信息接收部接收到的第二密钥信息，与通信对方的所述通信终端的识别信息对应起来进行存储；和

终端间加密通信部，其利用由作为所述第二密钥信息接收部接收到的第二密钥信息的所述密钥或所述种信息生成的所述密钥，在与通信对方的所述通信终端之间进行加密通信；

所述通信支持服务器，

具有：

通信条件存储部，其对于每个所述通信终端，将该通信终端可实施的加密通信的通信条件，与该通信终端的识别信息对应起来进行存储；

密钥共享部，其在与所述通信终端之间，进行作为用于与该通信终端的加密通信的密钥的第一密钥的共享；

服务器侧第一密钥存储部，其将通过所述服务器侧的密钥共享部在所述通信终端之间已共享的第一密钥，与对应的有效期限一起，与所述通信终端的识别信息对应起来进行存储；

服务器测加密通信部，其利用所述第一密钥，与具有与该第一密钥对应的识别信息的通信终端进行加密通信；

共通通信条件提取部，其经由所述服务器－终端间加密通信部利用从所述通信终端接收到的通信开始请求内包含的 2 个所述通信终端的识别信息并参照所述通信条件存储部，将作为该 2 个通信终端共通的通信条件的共通通信条件提取出来；和

第二密钥信息生成部，其生成遵从所述抽出的所述共通通信条件的加密通信中所使用的第二密钥信息，并将已生成的第二密钥信息与所述共通通信条件一起，经由所述服务

器－终端间加密通信部，发送给所述 2 个通信终端的每一个；

所述通信终端的终端－服务器间加密通信部，当向所述通信支持服务器请求加密通信时，

当是与所述第一密钥对应的第一密钥的有效期限的经过之前时，利用该第一密钥，向所述通信支持服务器请求加密通信，

当是所述第一密钥的有效期限的经过之后时，或该第一密钥没有存储在所述终端－服务器间用的存储部时，让所述终端侧的密钥共享部，进行用于与所述通信支持服务器间的加密通信的所述第一密钥的共享，并利用新共享的所述第一密钥，向该所述通信支持服务器请求加密通信，

当所述通信支持服务器的服务器－终端间加密通信部，向所述通信终端请求加密通信时，

当是与该通信终端的识别信息对应的第一密钥的有效期限经过之前时， 利用与该通信终端的识别信息对应的所述第一密钥，向该通信终端请求加密通信，

当是与该通信终端的识别信息对应的第一密钥的有效期限经过之后时，或对应该通信终端的识别信息的第一密钥没有存储在所述第一密钥存储部时，让所述密钥共享部，进行所述第一密钥的共享，并采用新共享的第一密钥，向该通信终端请求加密通信。

通信支持服务器、通信支持方法、及通信支持系统

技术领域

[0001] 本发明涉及通过互联网等通信网进行加密通信的技术。

背景技术

[0002] 当通过网络在通信终端之间进行加密通信时，有时按以下步骤预先共享用于该加密通信的公共密钥，采用共享的公共密钥进行加密通信。开始通信的通信终端，取得通信对方的通信终端的公开密钥。然后，开始通信的通信终端，生成用于与通信对方的通信终端间的加密通信的公共密钥，并采用通信对方的通信终端的公开密钥对该公共密钥进行加密，并发送给通信对方的通信终端。通信对方的通信终端，从开始通信的通信终端接收以自身的公开密钥加密过的公共密钥，再以与自己的公开密钥对应的秘密密钥进行解密。由此，开始通信的通信终端，与通信对方的通信终端共享用于与通信对方的通信终端间的加密通信的公共密钥。

[0003] 在上述方法中，当开始通信的通信终端，与多个通信对方的通信终端的各自进行加密通信时，需要与各个通信对方的通信终端共享用于加密通信的公共密钥，故有时开始通信的通信终端处理负荷变大。所以，在 Mark Baughter 等 3 名，“MSEC Group Key Management Architecture<draft-ietf-msec-gkmarch-07txt>”，IETF(Internet Engineering Task Force)，P3-13，http//www.left.org/internet-drafts/draft-ietf-msec-gkmarch-07.txt（以下称为非专利文献 1）中，公布了这样的技术，即在网络上设置将加密通信用的公共密钥分发给开始通信的通信终端与通信对方的通信终端的服务器，开始通信的通信终端与通信对方的通信终端，采用由该服务器分发的公共密钥，进行加密通信的技术。在该非专利文献 1 记载的技术中，服务器，生成开始通信的通信终端与通信对方的通信终端之间的加密通信用的公共密钥，并向开始通信的通信终端与通信对方的通信终端进行分发，由此，减轻了由开始通信的通信终端生成公共密钥而产生的处理负荷。

[0004] 但是，在加密通信的方式中，有多个种类，在各个种类的加密通信中，有时也有多个版本。因此，有时开始通信的通信终端及通信对方的通信终端，不支持依据由服务器分发的公共密钥的加密通信。由此，即使是由服务器发放了公共密钥，有时开始通信的通信终端与通信对方的通信终端也不能开始进行加密通信。

[0005] 另外，当通信终端开始与通信对方通信时，通信终端需要按照规定的认证步骤确认通信对方的合法性。然而，如果通信终端，与多个通信对方进行加密通信时，需要分别认证通信对方来确认合法性，有时通信终端的处理负荷会增大。

发明内容

[0006] 本发明鉴于上述情况形成的，提供一种即使是在多个种类的加密通信方式存在时，在通信终端之间，也能确实开始加密通信的技术。另外，本发明还提供一种降低通信终端进行认证步骤所需的处理负荷的技术。

[0007] 在本发明中，通信支持服务器，当与通信终端之间进行信息收发时，如果与该通信终端的识别信息对应起来而在第一密钥存储部存储的第一密钥是在有效期经过之前，就采用与该通信终端的识别信息对应起来存储在第一密钥存储部内的，用于与该通信终端进行加密通信之密钥的第一密钥，在与该通信终端之间进行加密通信，如果与该通信终端的识别信息对应起来并存储在第一密钥存储部的第一密钥是在有效期经过之后，或与该通信终端的识别信息对应起来的第一密钥没有存储在第一密钥存储部，就让密钥共享部，进行用于与该通信终端间的加密通信的第一密钥的共享，并采用新共享的第一密钥与该通信终端进行加密通信。

[0008] 例如，本发明提供一种通信支持服务器，它是支持通信终端之间加密通信的通信支持服务器，配备：对于每个通信终端，将该通信终端可实施加密通信的通信条件，与该通信终端的识别信息对应起来存储的通信条件存储部；在通信终端之间，将作为用于与该通信终端的加密通信的密钥的第一密钥进行共享的密钥共享部；将通过密钥共享部在通信终端之间进行共享的第一密钥，与对应的有效期一起，与通信终端的识别信息对应起来存储的第一密钥存储部；采用第一密钥存储部存储的第一密钥，与具有与第一密钥对应起来存储在第一密钥存储部的识别信息的通信终端进行加密通信的加密通信部；利用经由加密通信部从通信终端接收到的通信开始请求内所包含的 2 个通信终端的识别信息，并参照通信条件存储部，将作为该 2 个通信终端共通的通信条件的共通通信条件提取出来的共通通信条件提取部；生成作为在依据共通通信条件提取部提取出来的共通通信条件的加密通信中所采用的密钥的或用来算出该密钥的种信息的第二密钥信息，并将生成的第二密钥信息与共通通信条件一起，经由加密通信部发送给 2 个通信终端的每一个的第二密钥信息生成部；加密通信部，当在通信终端之间收发信息时，如果与该通信终端的识别信息对应起来存储在第一密钥存储部的第一密钥是在有效期经过之前，就采用与该通信终端的识别信息对应起来存储在第一密钥存储部内的第一密钥，在该通信终端之间进行加密通信，如果与该通信终端的识别信息对应起来存储在第一密钥存储部的第一密钥是在有效期经过之后，或与该通信终端的识别信息对应的第一密钥没有存储在第一密钥存储部，就让密钥共享部，进行用于该通信终端的加密通信的第一密钥的共享，并采用新共享的第一密钥与该通信终端进行加密通信。

[0009] 依据本发明，通信终端根据自己支持的通信条件，可以确实地与通信对方的终端开始通信。另外，本发明，能减轻与生成加密密钥有关的通信终端的负荷。而且，本发明，可降低有关认证过程的通信终端的处理负荷。

附图说明

[0010] 图 1 是表示本发明的一个实施方式的通信支持系统 10 的构成；

[0011] 图 2 是表示通信支持服务器 20 的一个构成例的方块图；

[0012] 图 3 是表示在加密密钥存储部 200 内存储的数据构造的一个例子；

[0013] 图 4 是表示在通信条件存储部 204 存储的数据构造的一个例子；

[0014] 图 5 是表示信息处理装置 14 的构成的一个例的方块图；

[0015] 图 6 是表示在加密密钥存储部 142 内存储的数据构造的一个例子；

[0016] 图 7 是表示在通信条件存储部 148 内存储的数据构造的一个例子；

[0017] 图 8 是表示在加密密钥存储部 158 内存储的数据构造的一个例子；

[0018] 图 9 是表示通信支持服务器 20 的一个动作例的流程图；

[0019] 图 10 是表示信息处理装置 14 在向通信支持服务器 20 或其他的信息处理装置 14 进行访问时信息处理装置 14 的一个动作例的流程图；

[0020] 图 11 是表示从通信支持服务器 20 或其他信息处理装置 14 访问信息处理装置 14 时的信息处理装置 14 的一个动作例的流程图。

[0021] 图 12 是用来说明信息处理装置 14 与多个其他信息处理装置 14 进行通信动作的顺序图；

[0022] 图 13 是表示可以实现通信支持服务器 20 或信息处理装置 14 的电子计算机 30 的硬件构成的一个例子。

具体实施方式

[0023] 以下，说明本发明的实施方式。

[0024] 图 1，表示本发明的一个实施方式的通信支持系统 10 的构成。通信支持系统 10，配备通信支持服务器 20 及多个信息处理装置 14。多个信息处理装置 14 的各自是，例如通用计算机、移动电话、或 IP(Internet Protocol) 电话等通信终端、或电子认证服务器或电子签名验证服务器等提供服务的服务器等。多个信息处理装置 14，连接因特网等通信网 12，经由通信网 12 相互进行通信。另外，各信息处理装置 14，经由通信网 12，与同样连接在通信网 12 的通信支持服务器 20 进行通信。

[0025] 在这里，在多个信息处理装置 14 中，当 2 个信息处理装置 14 经由通信网 12 互相进行通信时，在通信网 12 内流动的通信数据，有时被其他信息处理装置 14 获得，而泄漏通信内容。为了避免这种情况，有时要在该 2 个信息处理装置 14 之间对彼此的通信数据进行加密。

[0026] 另外，各信息处理装置 14，有时支持不同方式与不同版本的多个加密方式。如果通信源及通信对方的信息处理装置 14 支持的加密通信方式不同，通信对方的信息处理装置 14，有时不能对通信源的信息处理装置 14 支持的加密方式而加密的通信数据进行解密。因此，有时不能适当地进行加密通信。所以，在本实施方式中，信息处理装置 14，在通信支持服务器 20 要预先将信息处理装置 14 支持的通信条件进行登录，当通信源的信息处理装置 14 开始与通信对方的信息处理装置 14 通信时，根据自己及通信对方的信息处理装置 14 中共通的通信条件，使通信支持服务器 20 发行用于加密的公共密钥等加密密钥。由此，通信源的信息处理装置 14 与通信对方的信息处理装置 14 就能适当地开始加密通信。下面，对其细节进行说明。

[0027] 图 2，是表示通信支持服务器 20 的一个构成例的方块图。配备：通信支持服务器 20、加密密钥存储部 200、密钥共享部 202、通信条件存储部 204、通信条件受理部 206、加密通信部 208、通信开始请求接收部 210、通信条件提取部 212、密钥发放控制部 214、以及密钥信息生成部 216。密钥共享部 202，在与各个信息处理装置 14 之间，依据认证等预先确定的步骤，进行作为根据预先确定的加密通信方式的加密密钥的第一密钥的共享。

[0028] 加密密钥存储部 200，将密钥共享部 202 与信息处理装置 14 共享的各个第一密钥，与第一密钥的有效期一起，与信息处理装置 14 的识别信息对应起来存储。

[0029] 加密通信部 208，当利用信息处理装置 14 识别信息由信息处理装置 14 访问时，根据该识别信息参照加密密钥存储部 200，判定有效期内的第一密钥是否与该识别信息对应起来被存储在加密密钥存储部 200 内。当与该识别信息对应起来有效期内的第一密钥存储在加密密钥存储部 200 内时，加密通信部 208，就将与该识别信息对应起来的第一密钥从加密密钥存储部 200 读出，利用该第一密钥将从信息处理装置 14 接收到的数据解密后发送给通信条件受理部 206、通信开始请求接收部 210、以及密钥发放控制部 214。当有效期内的第一密钥没有与该识别信息对应起来存储在加密密钥存储部 200 内时，加密通信部 208，就让密钥共享部 202 在与信息处理装置 14 之间进行第一密钥的共享处理。

[0030] 另外，加密通信部 208，当向信息处理装置 14 进行访问时，在向信息处理装置 14 进行访问之前，根据访问目标的信息处理装置 14 的识别信息，参照加密密钥存储部 200，判断有效期内的第一密钥有没有与该识别信息对应起来存储在加密密钥存储部 200 内。如果有效期内的第一密钥与该识别信息对应起来存储在加密密钥存储部 200 内，加密通信部 208，就将与该识别信息对应起来的第一密钥从加密密钥存储部 200 读出，用该第一密钥，对发送给信息处理装置 14 的数据进行加密，经由通信网 12 发送给信息处理装置 14。当有效期内的第一密钥没有与该识别信息对应起来存储在加密密钥存储部 200 内时，加密通信部 208，就让密钥共享部 202 在与信息处理装置 14 之间进行第一密钥的共享处理。

[0031] 这样，通信支持服务器 20，当有效期内的第一密钥存储在加密密钥存储部 200 内时，就省略密钥共享部 202 所进行的第一密钥的共享处理。由此，通信支持服务器 20，与每次与信息处理装置 14 通信时进行第一密钥的共享处理的构成相比，能迅速开始与各个信息处理装置 14 之间的通信。

[0032] 通信条件存储部 204，在每个信息处理装置 14，将该信息处理装置 14 支持的加密通信的通信条件与该信息处理装置 14 的识别信息对应起来存储。所谓通信条件，例如，是支持加密算法的种类、版本、密钥的长度等信息。通信条件受理部 206，从多个信息处理装置 14 的各自，经由加密通信部 208，与各个信息处理装置 14 的识别信息一起，接受信息处理装置 14 各自的通信条件。然后，通信条件受理部 206，将接受的通信条件，与对应的该信息处理装置 14 的识别信息对应起来被存储在通信条件存储部 204 内。

[0033] 通信开始请求接收部 210，当接收到经由加密通信部 208 从各个信息处理装置 14 进行通信的、包含 2 个信息处理装置 14 的识别信息的通信开始请求时，就把接收到的通信开始请求发送给密钥发放控制部 214。另外，通信开始请求接收部 210，从将进行通信的 2 个信息处理装置 14 的识别信息，从接收到的通信开始请求提取出来，并将提取出来的信息处理装置 14 的识别信息发送给通信条件提取部 212。通信条件提取部 212，根据从通信开始请求接收部 210 接收到的 2 个信息处理装置 14 的识别信息参照通信条件存储部 204，将作为该 2 个信息处理装置 14 共通的通信条件的共通通信条件提取出来。

[0034] 密钥信息生成部 216，生成依照通信条件提取部 212 提取出来的共通通信条件的加密通信中所用的密钥的第二密钥，设定该第二密钥的有效期。然后，密钥信息生成部 216，将生成的第二密钥及有效期，与通信条件提取部 212 提取出来的共通通信条件一起发送给密钥发放控制部 214。另外，作为其他的例子，密钥信息生成部 216，生成用来算出依照通信条件提取部 212 提取的共通通信条件的加密通信中所采用的密钥的种信息的第二密钥信息，并设定该第二密钥信息的有效期，也可以将生成的第二密钥信息及有效期，与通信条件

提取部 212 提取出的共通通信条件一起发送给密钥发放控制部 214。

[0035] 密钥发放控制部 214，从由通信开始请求接收部 210 收到的通信开始请求中将进行通信的 2 个信息处理装置 14 的识别信息提取出来。然后，密钥发放控制部 214，向提取信息处理装置 14 的识别信息中、与通信对方的识别信息对应的信息处理装置 14，将密钥信息生成部 216 生成的第二密钥及有效期与通信开始请求一起经由加密通信部 208 进行发送。另外，密钥发放控制部 214，当经由加密通信部 208 接收到响应已发送的通信开始请求信息处理装置 14 返送了通信开始许可时，就参照接收到的通信开始许可中含有的信息处理装置 14 的识别信息，将密钥信息生成部 216 生成的第二密钥及有效期，与通信开始许可一起经由加密通信部 208，向发送了通信开始请求的信息处理装置 14 发送。

[0036] 这样，通信支持服务器 20，根据共通的通信条件生成第二密钥，并将生成的第二密钥，经由通信网 12 向对应的信息处理装置 14 发送。因此，与生成加密密钥，并将已生成的加密密钥仅向各个信息处理装置 14 发放的构成相比，不会发放依据信息处理装置 14 不支持的通信条件的加密密钥，信息处理装置 14，用从通信支持服务器 20 发放的加密密钥，能与其他的信息处理装置 14 确实地开始加密通信。

[0037] 图 3，是表示加密密钥存储部 200 存储的数据构造的一个例子。加密密钥存储部 200，是将作为用于一对终端之间加密通信的加密密钥的第一密钥 2002 及作为能够持续使用该第一密钥 2002 的期限的有效期 2004，与识别信息 2000 对应起来进行存储。

[0038] 另外，通过参照加密密钥存储部 200，加密通信部 208，被信息处理装置 14 访问时，当有对应该信息处理装置 14 的识别信息的、有效期内的第一密钥时，就将对应该识别信息的第一密钥，从加密密钥存储部 200 读出，可以用读出的第一密钥在与进行访问来的信息处理装置 14 之间进行加密通信。另一方面，当对应信息处理装置 14 的、有效期内的第一密钥在加密密钥存储部 200 内没有时，加密通信部 208，就可以让密钥共享部 202，在与进行访问来的信息处理装置 14 之间进行第一密钥的共享处理。

[0039] 再者，作为其他的例子，通信支持服务器 20，也可以具有利用通信支持服务器 20 带有的计时时刻的功能，将过了有效期的第一密钥从加密密钥存储部 200 删除的单元。在这种情况下，加密通信部 208，只要判断对应来访问过的或要访问的信息处理装置 14 的第一密钥是否被存储在了加密密钥存储部 200 就可以了，而不需要验证第一密钥的有效期，从而能更高速地开始与信息处理装置 14 的加密通信。

[0040] 图 4，是表示通信条件存储部 204 存储的数据构造的一个例子。通信条件存储部 204，将多个通信条件 2042 及对应该多个通信条件 2042 的优先级 2044，与识别信息 2040 对应起来存储。通过参照通信条件存储部 204，通信条件提取部 212，可提取在 2 个信息处理装置 14 中共通的通信条件。

[0041] 另外，在 2 个信息处理装置 14 的通信条件内，当多个共通的通信条件存在时，通信条件提取部 212，在多个共通通信条件中，就将例如为发送了通信开始请求的信息处理装置 14 的通信条件，且优先级最高的通信条件作为共通通信条件而提取出来。由此，信息处理装置 14，就能够实现例如，发送了与削减处理时间相比更希望提高加密强度的场合、或即使多少牺牲一些加密强度而更希望削减处理时间的场合等通信开始请求的、适应了信息处理装置 14 的偏好的终端间的加密通信。

[0042] 再者，当共通的通信条件在通信条件存储部 204 内不存在时，通信条件提取部

212，例如，作为共通通信条件，例如提取 NULL 数据。当通信条件提取部 212 提取了 NULL 数据时，密钥信息生成部 216，就将通信条件提取部 212 提取的 NULL 数据发送给密钥发放控制部 214。密钥发放控制部 214，如果从密钥信息生成部 216 接收了 NULL 数据，就将共通的通信条件不存在的意思，经由加密通信部 208 通知给发送了通信开始请求的信息处理装置 14。

[0043] 图 5，是表示信息处理装置 14 的一个构成例的方块图。信息处理装置 14，配备 :密钥共享部 140、加密密钥存储部 142、加密通信部 144、通信条件登录部 146、通信条件存储部 148、通信开始请求发送部 150、通信数据处理部 152、加密密钥接收部 154、加密通信部 156、以及加密存储部 158。

[0044] 密钥共享部 140，在与通信支持服务器 20 之间，按照预先确定的认证等步骤，进行第一密钥的共享。加密密钥存储部 142，将密钥共享部 140 与通信支持服务器 20 共享的第一密钥，与该第一密钥的有效期对应起来存储。

[0045] 加密通信部 144，当被通信支持服务器 20 访问时，参照加密密钥存储部 142，判断有效期内的第一密钥加密密钥是否存储在加密密钥存储部 142 内。如果有效期内的第一密钥存储在加密密钥存储部 142 内，加密通信部 144，就将该第一密钥从加密密钥存储部 142 读出，用该第一密钥把从通信支持服务器 20 接收到的通信数据解密并发送给加密密钥接收部 154。如果有效期内的第一密钥没有存储在加密存储部 142 内，加密通信部 144，就让密钥共享部 140 在与通信支持服务器 20 之间进行第一密钥的共享处理。此后，将该第一密钥从加密密钥存储部 142 读出，用该第一密钥把从通信支持服务器 20 接收到的通信数据解密并发送给加密接收部 154。

[0046] 另外，加密通信部 144，在访问通信支持服务器 20 时，在对通信支持服务器 20 的访问之前，参照加密密钥存储部 142，判定有效期内的第一密钥是否存储在加密密钥存储部 142 内。如果有效期内的第一密钥存储在加密密钥存储部 142 内，加密通信部 144，就从加密密钥存储部 142 读出该第一密钥。然后，加密通信部 144，用该第一密钥，把从通信条件登录部 146、通信开始请求发送部 150、以及加密密钥接收部 154 接收到的通信数据进行加密，经由通信网 12 发送给通信支持服务器 20。如果有效期内的第一密钥没有存储在加密密钥存储部 142 内，加密通信部 144，就让密钥共享部 140 在与通信支持服务器 20 之间进行第一密钥的共享处理。此后，用该第一密钥，把从通信条件登录部 146、通信开始请求发送部 150、以及加密密钥收信部 154 接收到的通信数据加密，并经由通信网 12 发送给通信支持服务器 20。

[0047] 通信条件存储部 148，存储信息处理装置 14 支持的通信条件。通信条件登录部 146，参照通信条件存储部 148，在通信条件被变更了时，就把信息处理装置 14 支持的通信条件从通信条件存储部 148 读出，经由加密通信部 144 发送给通信支持服务器 20。再者，在本例中，通信条件登录部 146，即使所支持的通信条件的一部分被变更或追加了时，也将通信条件存储部 148 存储的全部的通信条件发送给通信支持服务器 20。

[0048] 通信数据处理部 152，在生成通信对方的信息处理装置 14 的识别信息及应发送的通信数据的同时，处理经由加密通信部 156 接收到的通信数据。通信开始请求发送部 150，将通信数据处理部 152 生成的通信开始请求，与通信对方的信息处理装置 14 的识别信息以及自己的信息处理装置 14 的识别信息一起，经由加密通信部 144 发送给通信支持服务器

20。

[0049] 加密密钥收信部 154，将响应通信开始请求发送部 150 所发送的通信开始请求而从通信支持服务器 20 发送的通信开始许可，与根据自己以及由通信对方的信息处理装置 14 中共通的通信条件生成的第二密钥、共通通信条件、及有效期一起进行接收。然后，加密密钥接收部 154，从接收到的通信开始许可提取通信对方的信息处理装置 14 的识别信息，并将提取的识别信息，与从通信支持服务器 20 接收到的第二密钥、共通通信条件、以及有效期一起发送给加密密钥存储部 158。加密密钥存储部 158，将加密密钥接收部 154 从通信支持服务器 20 接收的第二密钥、共通通信条件、及有效期，与加密密钥接收部 154 从通信开始许可提取的通信对方的信息处理装置 14 的识别信息对应起来进行存储。

[0050] 另外，加密密钥接收部 154，如果从其他的信息处理装置 14 经由通信支持服务器 20 接收到通信开始请求时，就将该通信开始请求通知给通信数据处理部 152。通信数据处理部 152，在从加密密钥接收部 154 接收了通信开始请求时，就判断是否在与发送该通信开始请求的信息处理装置 14 之间进行加密通信。在与发送了该通信开始请求的信息处理装置 14 之间进行加密通信时，通信数据处理部 152，就让加密密钥接收部 154，向发送了通信开始请求的信息处理装置 14 经由加密通信部 144 返送通信开始许可。另一方面，在与发送该通信开始请求的信息处理装置 14 之间不进行加密通信时，通信数据处理部 152，就让加密密钥收信部 154，向发送通信开始请求的信息处理装置 14 经由加密通信部 144 返送不准许通信开始的意思。另外，加密密钥接收部 154，在接收到响应通信开始请求而不准许其他信息处理装置 14 发送的通信开始的意思时，就将其意思通知通信数据处理部 152。

[0051] 加密通信部 156，在通信数据处理部 152 从应用软件接收通信的要求而生成了应发送的通信数据时，就从通信数据处理部 152 接收该通信数据及通信对方的信息处理装置 14 的识别信息。然后，加密通信部 156，根据从通信数据处理部 152 接收到的通信对方的信息处理装置 14 的识别信息，参照加密密钥存储部 158，判断有效期内的第二密钥是否与该识别信息对应起来存储在加密密钥存储部 158 内。当有效期内的第二密钥与该识别信息对应起来存储在加密密钥存储部 158 内时，加密通信部 156，就将对应该识别信息的第二密钥及共通通信条件从加密密钥存储部 158 读出。然后，加密通信部 156，按照读出的共通通信条件所存储的加密算法或版本等的信息，由读出的第二密钥，将从通信数据处理部 152 接收到的通信数据加密，并经由通信网 12 发送给通信对方的信息处理装置 14。另一方面，当有效期内的第二密钥没有与该识别信息对应起来存储在加密密钥存储部 158 内时，加密通信部 156，就将需要从通信支持服务器 20 接收第二密钥的发放的意思通知给通信数据处理部 152。一接到这个通知，通信数据处理部 152，就让通信开始请求发送部 150 将通信开始请求发送给通信支持服务器 20。

[0052] 另外，加密通信部 156，当经由通信网 12 从该信息处理装置 14 接收到通信数据时，就根据接收到的通信数据中含有的通信对方的信息处理装置 14 的识别信息参照加密密钥存储部 158，判断有效期内的第二密钥是否与该识别信息对应起来存储在加密密钥存储部 158 内。当有效期内的第二密钥与该识别信息对应起来存储在加密密钥存储部 158 内时，加密通信部 156，就将对应该识别信息的第二密钥及共通通信条件从加密密钥存储部 158 读出，并根据读出的共通通信条件及对应的第二密钥，将从通信数据处理部 152 接收的通信数据解密，并发送给通信数据处理部 152。

[0053] 另一方面，当有效期内的第二密钥没有与该识别信息对应起来存储在加密密钥存储部 158 内时，加密通信部 156，就将需要从通信支持服务器 20 接收第二密钥的发放的意思通知给发送通信数据的信息处理装置 14。发送数据的信息处理装置 14，在通信数据处理部 152，一旦接到这个通知，就让通信开始请求发送部 150 将通信开始请求发送给通信支持服务器 20。

[0054] 再者，作为其他的例子，信息处理装置 14，也可以具有利用信息处理装置 14 拥有的计时时刻的功能，将过了有效期的第一密钥从加密密钥存储部 142 删除的单元。在这种情况下，加密通信部 144，在被通信支持服务器 20 访问了时，或要对通信支持服务器 20 进行访问时，只要判断第一密钥是否存储在加密密钥存储部就可以了，没有必要验证第一密钥的有效期，故能更高速地开始与通信支持服务器 20 的加密通信。

[0055] 图 6，是表示加密密钥存储部 142 存储的数据构造的一个例子。加密密钥存储部 142，将作为用于服务器间的加密通信的加密密钥的第一密钥 1422 及表示能持续使用该第一密钥 1422 的期限的有效期 1424，与通信支持服务器 20 的识别信息 1420 对应起来进行存储。通过参照加密密钥存储部 142，加密通信部 144，用第一密钥可在与通信支持服务器 20 之间进行加密通信。另外，在对通信支持服务器 20 访问或被通信支持服务器 20 访问了的任意一种情况下，通过参照加密密钥存储部 142，加密通信部 144，如果有有效期内的第一密钥，就能用该第一密钥在与通信支持服务器 20 之间进行加密通信。另一方面，当没有有效期内的第一密钥时，加密通信部 144，就让密钥共享部 140 在与通信支持服务器 20 之间进行第一密钥的共享处理。

[0056] 图 7，是表示通信条件存储部 148 存储的数据构造的一个例子。通信条件存储部 148，将优先级 1482 与自己的信息处理装置 14 支持的通信条件 1480 对应起来存储。通过参照通信条件存储部 148，通信条件登录部 146，可将对应优先级的通信条件登录处理，在通信支持服务器 20 的通信条件存储部 204 内。通过该登录处理，通信条件提取部 212，参照通信条件存储部 204，根据优先级可提取共通的通信条件。由此，通信支持系统 10，能实现适应发送了通信开始请求的信息处理装置 14 的偏好的终端间加密通信。

[0057] 图 8，是表示加密密钥存储部 158 存储的数据构造的一个例子。加密密钥存储部 158，将通信对方的信息处理装置 14 之间的加密通信中用的第二密钥 1582、作为自己及通信对方的信息处理装置 14 中共通的通信条件的共通通信条件 1584、第二密钥 1582 及共通通信条件 1584、作为能持续使用的期限的有效期 1586，与作为识别通信对方的信息处理装置 14 的信息的通信对方的识别信息 1580 对应起来存储。加密通信部 156，通过参照加密密钥存储部 158，可判定用于加密在与通信对方的信息处理装置 14 之间收发的数据的有效期内的第二密钥是否存储在加密密钥存储部 158 内。

[0058] 图 9，是表示通信支持服务器 20 的一个动作例的流程图。在电源投入等规定的定时，通信支持服务器 20，开始本流程图所示的处理。首先，加密通信部 208，判断是否被信息处理装置 14 访问了 (S100)。当没有被信息处理装置 14 访问时 (S100 :No)，加密通信部 208，就在被信息处理装置 14 访问之前重复步骤 100。

[0059] 在步骤 100 中，当被信息处理装置 14 访问了时 (S100 :Yes)，加密通信部 208，就判定是否是要求共享第一密钥的通信数据 (S102)。当是要求共享第一密钥的通信数据 (S102 :Yes)，加密通信部 208，就让密钥共享部 202，在与来访问的信息处理装置 14 之间进

行第一密钥的共享处理 (S104)，再次进行步骤 100 所示的处理。

[0060] 在步骤 104 中，密钥共享部 202，例如，从信息处理装置 14 的密钥共享部 140 接收服务器 - 终端之间加密通信中用的一个以上的候选参数。然后，密钥共享部 202，从接收到的候选参数中，选择一个加密通信部 208 支持的参数，返送给共享部 140，这样，在与密钥共享部 140 之间共享加密通信中用的参数。然后，密钥共享部 202，在将通信支持服务器 20 的公开密钥证明书发送给密钥共享部 140 的同时，向密钥共享部 140 要求信息处理装置 14 的公开密钥证明书。然后，密钥共享部 202，通过验证从密钥共享部 140 接收到的公开密钥证明书的有效期、签名，来验证公开密钥证明书。

[0061] 当公开密钥证明书验证成功了时，密钥共享部 202 与密钥共享部 140，就将共享的参数与参数的电子签名一起发送给通信对方，通过验证接收的电子签名，来认证通信对方。然后，当密钥共享部 202 与密钥共享部 140 相互的认证成功了时，密钥共享部 140，就根据共享的参数，生成与通信支持服务器 20 的加密通信部 208 间的加密通信中用的第一密钥。然后，密钥共享部 140，通过将生成的第一密钥用通信支持服务器 20 的公开密钥加密后发送到密钥共享部 202，共享在与密钥共享部 202 之间加密通信中用的第一密钥。

[0062] 再者，密钥共享部 202，也可以将从密钥共享部 140 接收到的公开密钥证明书的验证，委托给在外部设立的验证服务器。验证服务器，当被密钥共享部 202 委托了公开密钥证明书的验证时，在验证公开密钥证明书的有效期、签名的同时，探寻该公开密钥证明书记载的认证局，从到达的认证局得到该公开密钥证明书的失效信息，通过验证得到的失效信息，来验证公开密钥证明书。由此，密钥共享部 202，能更严密地验证信息处理装置 14 的公开密钥证明书。

[0063] 在步骤 102 中，当接收的通信数据不是要求共享第一密钥的通信数据时 (S102 ：No)，加密通信部 208，就根据来访问的信息处理装置 14 的识别信息参照加密密钥存储部 200，判断有效期内的第一密钥是否与该识别信息对应起来存储在加密密钥存储部 200 内 (S106)。当有效期内的第一密钥没有与该识别信息对应起来存储在加密密钥存储部 200 内时 (S106 ：No)，加密通信部 208，就让密钥共享部 202，将需要进行第一密钥的共享处理的意思通知给来访问的信息处理装置 14(S128)，再次进行步骤 100 所示的处理。

[0064] 在步骤 106 中，当有效期内的第一密钥与该识别信息对应起来存储在加密密钥存储部 200 内时 (S106 ：Yes)，加密通信部 208，就从加密密钥存储部 200 读出对应的第一密钥，并用读出的第一密钥将接收到的通信数据解密。然后，加密通信部 208，将解密过的通信数据发送给通信条件受理部 206、通信开始请求接收部 210、及密钥发放控制部 214(S108)。接着，通信条件受理部 206，判断接收到的通信数据是不是要求登录通信条件的数据还是其他 (S110)。在接收到的通信数据是要求登录通信条件的数据时 (S110 ：通信条件登录)，通信条件受理部 206，就将接收到的通信数据中含有的通信条件，与发送了该通信数据的信息处理装置 14 的识别信息对应起来存储在通信条件存储部 204 内 (S112)，加密通信部 208，再次进行步骤 100 所示的处理。

[0065] 如果接收到的通信数据是要求登录通信条件的数据以外的数据时 (S110 ：除此之外)，通信开始请求收信部 210 及密钥发放控制部 214，就判定接收到的通信数据是表示通信开始请求的数据，还是表示响应通信开始请求而返送的通信开始许可的数据 (S114)。如果接收到的通信数据是表示通信许可的数据时 (S114 ：通信许可)，密钥发放控制部 214，就

将密钥信息生成部 216 生成的第二密钥、共通通信条件、及该第二密钥的有效期，与通信开始许可一起，经由加密通信部 208，发送给发送了通信开始请求的信息处理装置 14(S116)，加密通信部 208，再次进行步骤 100 所示的处理。

[0066] 在步骤 114 中，如果接收到的通信数据是表示通信开始请求的数据 (S 114 :通信开始请求)，通信开始请求接收部 210，就从接收到的通信开始请求提取进行通信的 2 个信息处理装置 14 的识别信息，并将提取的信息处理装置 14 的识别信息发送给通信条件提取部 212。然后，通信条件提取部 212，根据从通信开始请求收信部 210 收到的 2 个信息处理装置 14 的识别信息，参照通信条件存储部 204，提取作为该 2 个信息处理装置 14 中共通的通信条件的共通通信条件 (S118)。

[0067] 接着，密钥信息生成部 216，生成在按照通信条件提取部 212 提取的共通通信条件的加密通信中所用的第二密钥，并设定该第二密钥的有效期。然后，密钥信息生成部 216，将生成的第二密钥及有效期，与由通信条件提取部 212 提取的共通通信条件一起发送给密钥发放控制部 214。密钥发放控制部 214，从由通信开始请求接收部 210 接收到的通信开始请求提取进行通信的 2 个信息处理装置 14 的识别信息。然后，密钥发放控制部 214，将提取的信息处理装置 14 的识别信息内、通信对方的信息处理装置 14 的识别信息作为目的地，将由密钥信息生成部 216 生成的第二密钥及有效期，以及由通信条件提取部 212 提取的共通通信条件，与通信开始请求一起发送给加密通信部 208(S120)。

[0068] 接着，加密通信部 208，根据从密钥发放控制部 214 作为目的地而接收到的信息处理装置 14 的识别信息，参照加密密钥存储部 200，判断有效期内的第一密钥是否与该识别信息对应起来存储在加密密钥存储部 200 内 (S122)。如果有效期内的第一密钥与该识别信息对应起来存储在加密密钥存储部 200 内 (S122 :Yes)，加密通信部 208，就从加密密钥存储部 200 读出对应的第一密钥。然后，加密通信部 208，用读出的第一密钥，将从密钥发放控制部 214 接收到的第二密钥及有效期，以及由通信条件提取部 212 提取的共通通信条件，与通信开始请求一起进行加密后，发送给通信对方的信息处理装置 14(S126)，加密通信部 208，再次进行步骤 100 所示的处理。

[0069] 在步骤 122 中，当有效期内的第一密钥没有与该识别信息对应起来存储在加密密钥存储部 200 内时 (S122 :No)，加密通信部 208，就让密钥共享部 202，在与通信对方的信息处理装置 14 之间，进行第一密钥的共享处理 (S124)，进行步骤 126 所示的处理。

[0070] 图 10，是表示信息处理装置 14 访问通信支持服务器 20 或其他信息处理装置 14 时的、信息处理装置 14 的一个动作例的流程图。在电源投入等规定的定时，信息处理装置 14，开始本流程图所示的处理。首先，通信数据处理部 152，判断应该发送的通信数据是否发生了 (S200)。当应该发送的通信数据发生了时 (S200 :Yes)，加密通信部 156，就从通信数据处理部 152 接收该通信数据及通信对方的信息处理装置 14 的识别信息。然后，加密通信部 156，根据接收到的通信对方的信息处理装置 14 的识别信息，参照加密密钥存储部 158，判断有效期内的第二密钥是否与该识别信息对应起来存储在了加密部密钥存储部 158 内 (S202)。如果有效期内的第二密钥与该识别信息对应起来存储在了加密密钥存储部 158 内 (S202 :Yes)，则加密通信部 156，就从加密密钥存储部 158 读出对应的第二密钥。然后，加密通信部 156，用读出的第二密钥对从通信数据处理部 152 接收到的通信数据进行加密后，经由通信网 12 发送给通信对方的信息处理装置 14(S204)，通信数据处理部 152，再次进行

步骤 200 所示的处理。

[0071] 在步骤 202 中，如果有效期内的第二密钥没有与该识别信息对应起来存储在加密密钥存储部 158 内 (S202 :No)，则加密通信部 156，就将需要从通信支持服务器 20 接收第二密钥的发放的意思通知给通信数据处理部 152。一旦接到这个通知，通信数据处理部 152，就让通信开始请求发送部 150 将通信开始请求，经由加密通信部 144 发送给通信支持服务器 20。在这种情况下，加密通信部 144，判断有效期内的第一密钥是否存储在加密密钥存储部 142 内 (S206)。如果有效期内的第一密钥存储在加密密钥存储部 142 内 (S206 :Yes)，加密通信部 144，就从加密密钥存储部 142 读出第一密钥。然后，加密通信部 144，用读出的第一密钥，对从通信开始请求发送部 150 接收到的通信开始请求进行加密后，经由通信网 12 发送给通信支持服务器 20(S210)，通信数据处理部 152，再次进行步骤 200 所示的处理。

[0072] 在步骤 206 中，如果有效期内的第一密钥没有存储在加密密钥存储部 142 内时 (S206 :No)，则加密通信部 144，就让密钥共享部 140，在与通信支持服务器 20 之间进行第一密钥的共享处理 (S208)，进行步骤 210 所示的处理。

[0073] 在步骤 200 中，当应发送通信数据没有发生时 (S200 :No)，通信条件登录部 146，参照通信条件存储部 148，判断通信条件存储部 148 中存储的通信条件是否被变更了 (S212)。当通信条件没有被变更时 (S212 :No)，通信数据处理部 152，再次进行步骤 200 所示的处理。

[0074] 在步骤 212 中，当通信条件被变更了时 (S212 :Yes)，通信条件登录部 146，就将通信条件存储部 148 中存储的通信条件全部读出。然后，通信条件登录部 146，生成包含读出的通信条件的通信条件登录要求，并将生成的通信条件登录要求发送给加密通信部 144。接着，加密通信部 144，判断有效期内的第一密钥是否存储在加密密钥存储部 142 内 (S214)。如果有效期内的第一密钥存储在加密密钥存储部 142 内 (S214 :Yes)，加密通信部 144，就从加密密钥存储部 142 读出第一密钥。然后，加密通信部 144 用读出的第一密钥，对从通信条件登录部 146 接收到的通信条件登录要求进行加密后，经由通信网 12 发送给通信支持服务器 20(S218)，通信数据处理部 152，再次进行步骤 200 所示的处理。

[0075] 在步骤 214 中，如果有效期内的第一密钥没有存储在加密密钥存储部 142 内 (S214 :No)，则加密通信部 144，就让密钥共享部 140，在与通信支持服务器 20 之间进行第一密钥的共享处理 (S216)，进行步骤 218 所示的处理。

[0076] 图 11，是表示当信息处理装置 14 被通信支持服务器 20 或其他信息处理装置 14 访问时的信息处理装置 14 的一个动作例的流程图。在投入电源等规定的定时，信息处理装置 14，开始本流程图所示的处理。首先，加密通信部 144 及加密通信部 156，判断是否被通信支持服务器 20 或其他信息处理装置 14 的任意一个访问了 (S300)。当没有被通信支持服务器 20 或其他信息处理装置 14 的任意一个访问时 (S300 :No)，重复步骤 300，直到加密通信部 144 及加密通信部 156 被通信支持服务器 20 或其他信息处理装置 14 的任意一个访问为止。

[0077] 在步骤 300 中，当有来自通信支持服务器 20 或其他信息处理装置 14 的任意一个的访问时 (S300 :Yes)，加密通信部 144 及加密通信部 156，就判断该访问是不是来自通信支持服务器 20 的 (S302)。如果该访问不是来自通信支持服务器 20 的，即该访问是来自其他信息处理装置 14 的时 (S302 :No)，加密通信部 156，根据经由通信网 12 与通信数据一起从其他信息处理装置 14 接收的信息处理装置 14 的识别信息，参照加密密钥存储部 158，判断

有效期内的第二密钥是否与该识别信息对应起来存储在加密密钥存储部 158 内 (S324)。当有效期内的第二密钥与该识别信息对应起来存储在加密密钥存储部 158 内时 (S324 :Yes)，加密通信部 156，就从加密密钥存储部 158 读出对应的第二密钥。然后，加密通信部 156，用读出的第二密钥，对从其他信息处理装置 14 接收到的通信数据进行解密后，在发送给通信数据处理部 152 的同时，如果对应接收到的通信数据有通信数据处理部 152 发送的通信数据，就对该数据进行加密后，经由通信网 12 返送给通信对方的信息处理装置 14(S326)，加密通信部 144 及加密通信部 156，再次进行步骤 300 所示的处理。

[0078] 在步骤 324 中，当有效期内的第二密钥没有与该识别信息对应起来存储在加密密钥存储部 158 内时 (S324 :No)，加密通信部 156，就向来访问的其他信息处理装置 14 返送需要从通信支持服务器 20 接收第二密钥的发放的意思 (S328)，加密通信部 144 及加密通信部 156，再次进行步骤 300 所示的处理。

[0079] 在步骤 302 中，如果有来自通信支持服务器 20 的访问时 (S302 :Yes)，加密通信部 144，就判断有效期内的第一密钥是否存储在加密密钥存储部 142 内 (S304)。如果有效期内的第一密钥存储在加密密钥存储部 142 内 (S304 :Yes)，则加密通信部 144，就用读出的第一密钥，对从通信支持服务器 20 接收到的数据进行解密 (S308)。如果有效期内的第一密钥没有存储在加密密钥存储部 142 内 (S304 :No)，则加密通信部 144，就让密钥共享部 140，在与通信支持服务器 20 之间进行第一密钥的共享处理 (S306)，进行步骤 308 所示的处理。

[0080] 步骤 306 的处理，是例外的处理，例如是由于通信支持服务器 20 与信息处理装置 14 间的内部时钟的偏差等而发生的处理。

[0081] 接着，加密密钥收信部 154，判断是从通信支持服务器 20 接收到的通信数据表示通信开始请求的数据，抑或还是响应通信开始请求经由通信支持服务器 20 返送的表示通信开始许可的数据 (S310)。如果接收到的通信数据是通信开始请求时 (S310 :通信开始请求)，加密密钥收信部 154，就把接收到的通信开始请求发送给通信数据处理部 152。然后，加密密钥收信部 154，与通信开始请求一起将接收到的第二密钥、共通通信条件、以及该第二密钥的有效期，与已发送的通信开始请求的信息处理装置 14 的识别信息对应起来存储在加密密钥存储部 158 内 (S312)。

[0082] 接着，通信数据处理部 152，判断是否要与发送来通信开始请求的信息处理装置 14 进行通信 (S318)。如果要与发送来通信开始请求的信息处理装置 14 进行通信 (S318 :Yes)，通信数据处理部 152，就让通信开始请求发送部 150 将通信开始许可经由加密通信部 144 发送给支持服务器 20(S322)，加密通信部 144 与加密通信部 156，再次进行步骤 300 所示的处理。在步骤 322 中，加密通信部 144，使用存储在加密密钥存储部 142 的第一密钥，对该通信开始许可进行加密后，经由通信网 12 发送给通信支持服务器 20。

[0083] 在步骤 318 中，当不与发送来通信开始请求的信息处理装置 14 进行通信时 (S318 :No)，通信数据处理部 152，就让通信开始请求发送部 150 将不准许通信开始的意思，经由加密通信部 144，发送给通信支持服务器 20(S320)，加密通信部 144 与加密通信部 156，再次进行步骤 300 所示的处理。

[0084] 在步骤 310 中，当接收的通信数据是通信开始许可时 (S310 :通信开始许可)，加密密钥接收部 154，就将接收到的通信开始许可发送给通信数据处理部 152。然后，加密密钥接收部 154，将与通信开始许可一起接收到的第二密钥及该第二密钥的有效期与发送了通

信开始许可的信息处理装置14的识别信息对应起来存储在加密密钥存储部158内(S314)。然后，加密通信部156，将与通信开始许可一起接收到的第二密钥从加密密钥存储部158读出。然后，加密通信部156，用读出的第二密钥，对通信数据处理部152生成的通信数据进行加密，经由通信网12，发送给其他信息处理装置14，同时，从其他信息处理装置14将经由通信网12接收到的通信数据解密后发送给通信数据处理部152(S316)。然后，加密通信部144与终端间加密通信部156，再次进行步骤300所示的处理。

[0085] 在这里，将图9、图10、及图11表示的各个处理的关系汇总如下。

[0086] 在进行加密通信的信息处理装置14之间，在有与通信对方的信息处理装置14对应的有效期内的第二密钥时，在图10的步骤204中，信息发送方的信息处理装置14用第二密钥对通信数据进行加密，并发送给通信对方的信息处理装置14。然后，在图11的步骤326中，加密通信部156，将信息接收方的信息处理装置14接收到的数据用第二密钥解密。此后，信息处理装置14，用对应的第二密钥进行加密通信。

[0087] 另外，当具有有效期内的第一密钥的信息处理装置14，向通信支持服务器20登录通信条件时，在图10的步骤218中，用第一密钥给通信条件加密并发送给通信支持服务器20。收到此后，通信支持服务器20，在图9的步骤112中，将接收的通信条件存储到通信条件存储部204。

[0088] 另外，当进行加密通信的信息处理装置14之间，没有与通信对方的信息处理装置14对应的有效期内的第二密钥、且没有在有效期内的第一密钥时，在图10的步骤208中，信息发送方的信息处理装置14，在与通信支持服务器20之间，进行第一密钥的共享处理。这个时候，通信支持服务器20，在图9的步骤104中，在与来访问的信息处理装置14之间进行第一密钥的共享处理。

[0089] 此后，信息发送方的信息处理装置14，在图10的步骤210中，用在与通信支持服务器20之间共享的第一密钥，对通信开始请求进行加密并发送给通信支持服务器20。收到此后，通信支持服务器20，在图9的步骤118及120中，根据进行加密通信的2个信息处理装置14的通信条件生成第二密钥。

[0090] 然后，通信支持服务器20，在图9的步骤124中，在与接收方的信息处理装置14之间进行第一密钥的共享处理。这个时候，接收方的信息处理装置14，在图11的步骤306中，在与通信支持服务器20之间进行第一密钥的共享处理。

[0091] 然后，通信支持服务器20，在图9的步骤126中，用共享的第一密钥对通信开始请求及第二密钥等进行加密，并发送给信息接收方的信息处理装置14。这个时候，接收方的信息处理装置14，在图11的步骤312中，将与通信开始请求一起接收到的第二密钥等进行存储，在步骤322中，用第一密钥对通信许可加密并发送给通信支持服务器20。收到此后，通信支持服务器20，在图9的步骤116中，用第一密钥对通信开始许可及第二密钥等进行加密，并发送给发送方的信息处理装置14。收到此后，发送方的信息处理装置14，在图11的步骤314及316中，将与通信开始许可一起接收到的第二密钥等进行存储，用存储的第二密钥，在与接收方的通知处理装置14之间进行加密通信。

[0092] 图12，是说明在第一密钥的有效期内与多个信息处理装置14进行的通信动作的顺序图。在图12所示的情况下，各个信息处理装置14的通信条件假定已经被登录在了通信支持服务器20。在与信息处理装置14-2间的加密通信之前，信息处理装置14-1，进行在

与通信支持服务器 20 之间的加密通信中用的第一密钥的共享处理 (S400)。然后，信息处理装置 14-1，将信息处理装置 14-2 的识别信息作为通信对方的识别信息的通信开始请求发送给通信支持服务器 20(S401)。

[0093] 接着，通信支持服务器 20，根据接收到的通信开始请求中含有的信息处理装置 14-1 及 14-2 的识别信息，提取两者共通的通信条件。然后，通信支持服务器 20，根据提取的共通通信条件，生成在信息处理装置 14-1 与信息处理装置 14-2 之间的加密通信中使用的第二密钥 (S402)。然后，通信支持服务器 20，与通信开始请求一起，将第二密钥及用来生成该第二密钥所参照过的共通通信条件发送给信息处理装置 14-2(S403)。这种情况下，在通信支持服务器 20 与信息处理装置 14-2 之间，当有效期内的第一密钥不存在时，就在通信支持服务器 20 与信息处理装置 14-2 之间，进行步骤 400 所示的第一密钥的共享处理。

[0094] 接着，信息处理装置 14-2，按照通信开始请求将通信开始许可向通信支持服务器 20 应答 (S404)。然后，通信支持服务器 20，将从信息处理装置 14-2 接收到的通信开始许可，与生成的第二密钥及共通通信条件一起发送给信息处理装置 14-1(S405)。然后，信息处理装置 14-1 与信息处理装置 14-2，用由通信支持服务器 20 发放的第二密钥及共通通信条件，就能互相进行加密通信 (S406)。

[0095] 在步骤 402 中，通信支持服务器 20，与第二密钥一起，生成能持续使用该第二密钥的期限的有效期，与第二密钥及共通通信条件一起，将生成的有效期分别发放给信息处理装置 14-1 及 14-2。为此，信息处理装置 14-1 与信息处理装置 14-2，如果是在该有效期内，如步骤 410 所示，就总能用第二密钥进行加密通信。

[0096] 另外，在步骤 400 中，将有效期也与信息处理装置 14-1 与通信支持服务器 20 共享的第一密钥对应起来，如果是在该有效期内，信息处理装置 14-1 与通信支持服务器 20，在步骤 400 中就能持续使用共享的第一密钥。因此，例如，当信息处理装置 14-1 与信息处理装置 14-3 进行加密通信时，在步骤 400 中，如果是在共享的第一密钥的有效期内，信息处理装置 14-1，就省略与通信支持服务器 20 的密钥共享处理，在步骤 400 中，就能从用共享的第一密钥、对给信息处理装置 14-3 的通信开始请求进行加密后、发送给通信支持服务器 20 的步骤开始进行处理 (S420)。

[0097] 通过以上动作，信息处理装置 14，当与多个其他信息处理装置 14 之间进行加密通信时，在与各个其他信息处理装置 14 之间，不需要进行第二密钥的共享处理，取而代之，只要在与通信支持服务器 20 之间，进行第一密钥的共享处理就行了。再者，信息处理装置 14，如果有在有效期内的第一密钥，就能省略第一密钥的共享处理。由此，信息处理装置 14，只要在与通信支持服务器 20 之间进行一次第一密钥的共享处理之后，如果有在有效期内的第一密钥，就不进行第一密钥的共享处理，能更迅速地开始与其他信息处理装置 14 的通信，能实现所谓的单一登录。

[0098] 图 13，是表示可以实现通信支持服务器 20 或信息处理装置 14 的电子计算机 30 的硬件构成的一个例子。电子计算机 30，配备 :CPU300、RAM301、ROM302、外部存储装置 303、通信接口 304、输出入装置 305、及媒体接口 306。

[0099] CPU300，根据存储在 RAM301 及 ROM302 的程序动作，进行各部分的控制。ROM302 及外部存储装置 303，存储在电子计算机 30 启动时 CPU300 执行的引导程序和依存于电子计算机 30 的硬件的程序等。RAM301，存储 CPU300 执行的程序及 CPU300 使用的数据等。

[0100] 通信接口 304，将经由通信网 12 从其他的电子计算机 30 接收到的程序和 / 或数据，提供给 RAM301 或外部存储装置 303，或发送给 CPU300。与此同时，通信接口 304，将 CPU300 生成的数据发送给其他的电子计算机 30。输出入装置 305，接收来自电子计算机 30 的管理者或用户的数据，在发送给 CPU300 的同时，还将 CPU300 生成的数据通知管理者和用户等。媒体接口 306，从记录媒体 307 读取程序和 / 或数据，并提供给 RAM301 或外部存储装置 303。

[0101] 上述程序，可以预先存储在 ROM302 或外部存储装置 303 内。或者，上述程序，根据需要，也可以从记录媒体 307 经由媒体接口 306 读出，并存储在 ROM302 或外部存储装置 303，还可以经由通信接口 304 与通信媒体，存储在 ROM302 或外部存储装置 303。

[0102] 在电子计算机 30 作为通信支持服务器 20 动作时，被安装在电子计算机 30 内可执行的程序，使电子计算机 30，分别作为下述部分来工作 ：即加密密钥存储部 200、密钥共享部 202、通信条件存储部 204、通信条件受理部 206、加密通信部 208、通信开始请求接收部 210、通信条件提取部 212、密钥发放控制部 214 及密钥信息生成部 216。

[0103] 另外，在电子计算机 30 作为信息处理装置 14 动作时，被安装在电子计算机 30 可执行的程序，使电子计算机 30，分别作为下述部分来工作 ：即密钥共享部 140、加密密钥存储部 142、加密通信部 144、通信条件登录部 146、通信条件存储部 148、通信开始请求发送部 150、通信数据处理部 152、加密密钥接收部 154、加密通信部 156、及加密密钥存储部 158。

[0104] 记录媒体 307，例如可以是 DVD、PD 等光学记录媒体、MD 等光磁记录媒体、磁带媒体、磁记录媒体、或半导体记录装置等。另外，通信媒体，例如可以是电缆、载波、及数字信号等。

[0105] 以上，用实施方式对本发明进行了说明，但本发明的技术范围不限于上述实施方式所述的范围。另外，对上述实施方式，可以附加各种各样的变更或改良，这对于业内人员来说是显而易见的。再者，由专利请求的范围的记述中明确看出，施加了那些变更或改良的形态也包含在本发明的技术范围中。

[0106] 例如，通信支持服务器 20 及信息处理装置 14 所拥有的多个功能块的各自，也可以分别通过 ASIC(Application Specific Integrated Circuit)，FPGA(Field Programmable Gate Array) 等的集成逻辑 IC 由硬件实现，或者，也可以通过 DSP(Digital Signal Processor) 或通用计算机在软件上实现。

[0107] 另外，在本例中，在通信条件存储部 204 内存储的各个信息处理装置 14 的通信条件，是从各个信息处理装置 14 经由通信网 12 来登录，而作为其他的例子，各个信息处理装置 14 的通信条件，也可以预先登录在通信条件存储部 204 内。

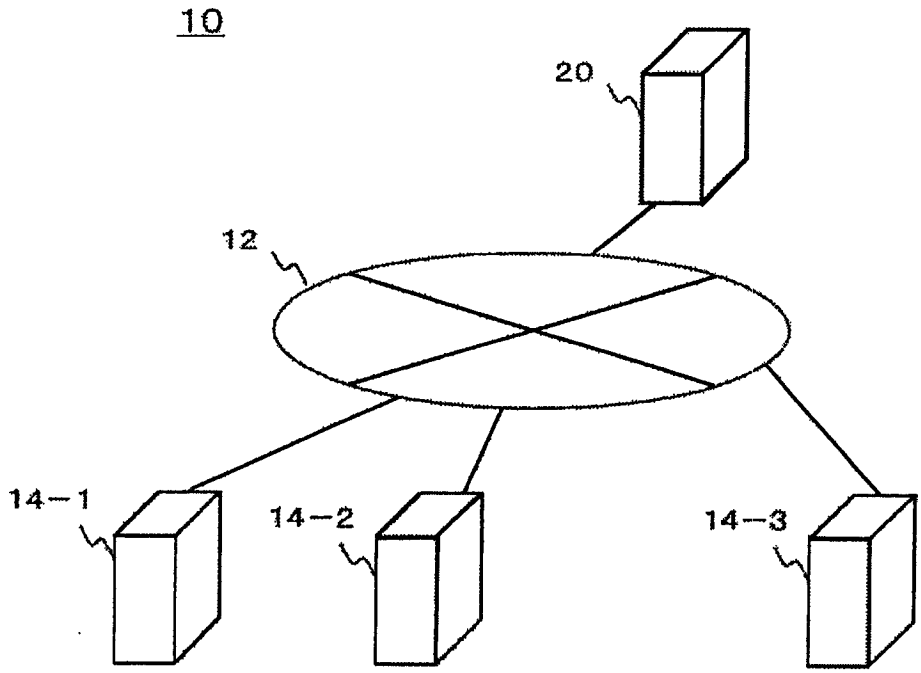

10
20
12
14－1
14－2
14－3

图 1

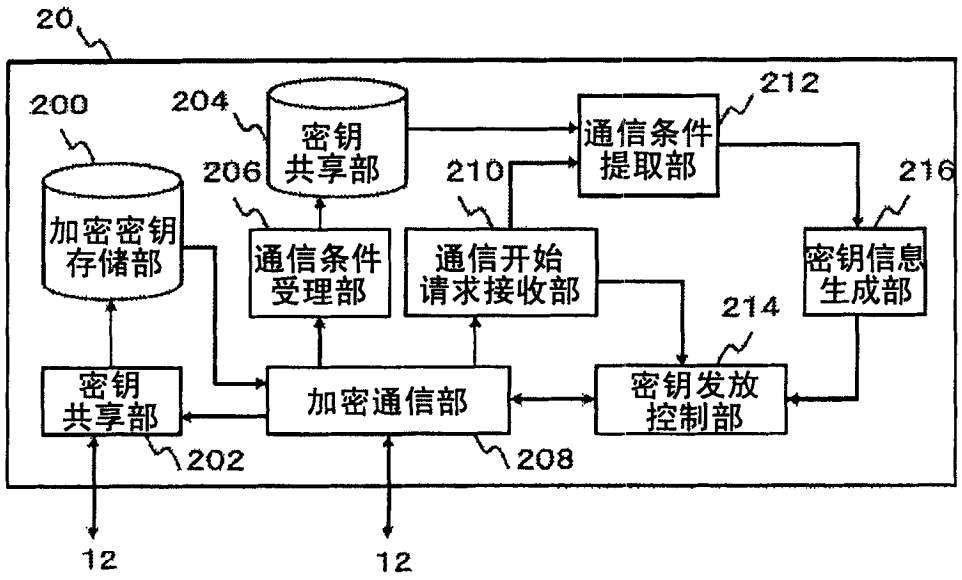

20
200
204
密钥
共享部
212
通信条件
提取部
206
210
216
加密密钥
存储部
通信条件
受理部
通信开始
请求接收部
密钥信息
生成部
214
密钥
共享部
加密通信部
密钥发放
控制部
202
208
12
12

图 2

200

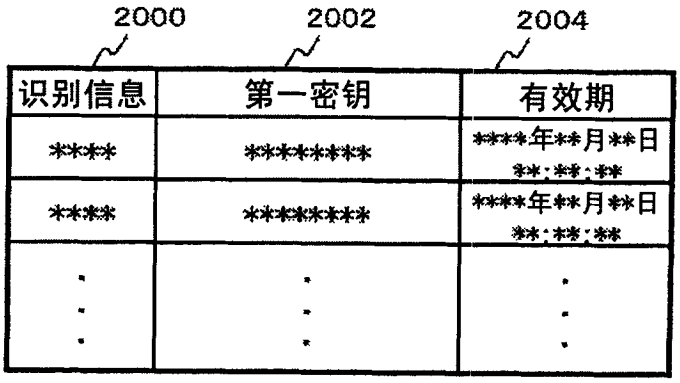

2000
2002
2004
识别信息
第一密钥
有效期
****
****
****年**月**日
::**
****
****
****年**月**日
::**

图 3

204

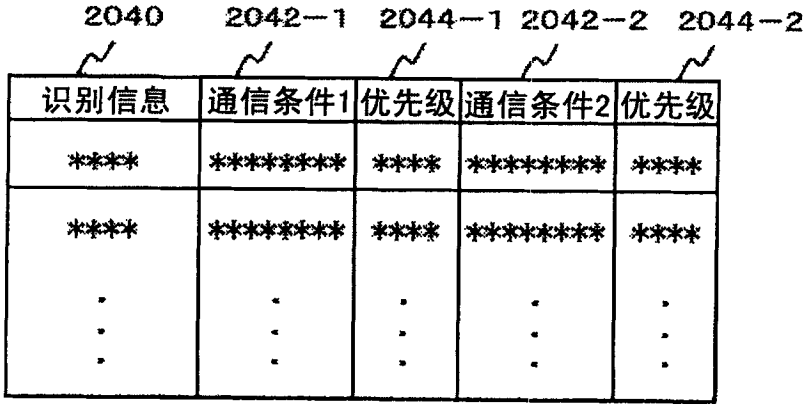

2040
2042—1
2044—1
2042—2
2044—2
识别信息
通信条件1
优先级
通信条件2
优先级
****
****
****
****
****
****
****
****
****
****

图 4

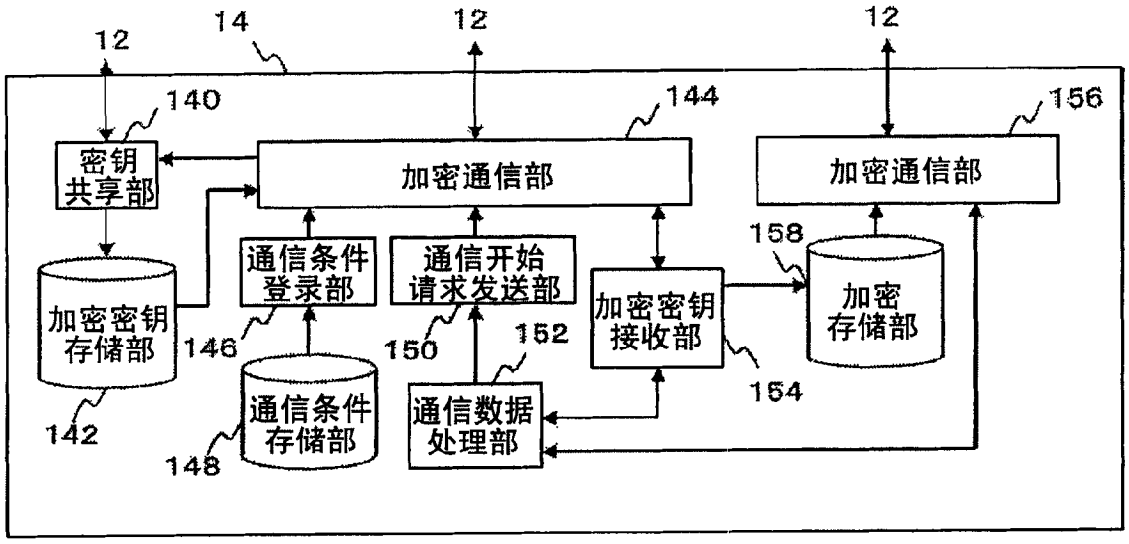


图 5

142

1420 识别信息	1422 第一密钥	1424 有效期
****	****	****年**月**日**:**:**

图 6

148

1480 通信条件	1482 优先级
*********	***
*********	***
.	.
.	.
.	.

图 7

158

1580 通信对方识别信息	1582 第二密钥	1584 共通通信条件	1586 有效期
****	****	****	****年**月**日**:**:**
****	****	****	****年**月**日**:**:**
⋮	⋮	⋮	⋮

图 8

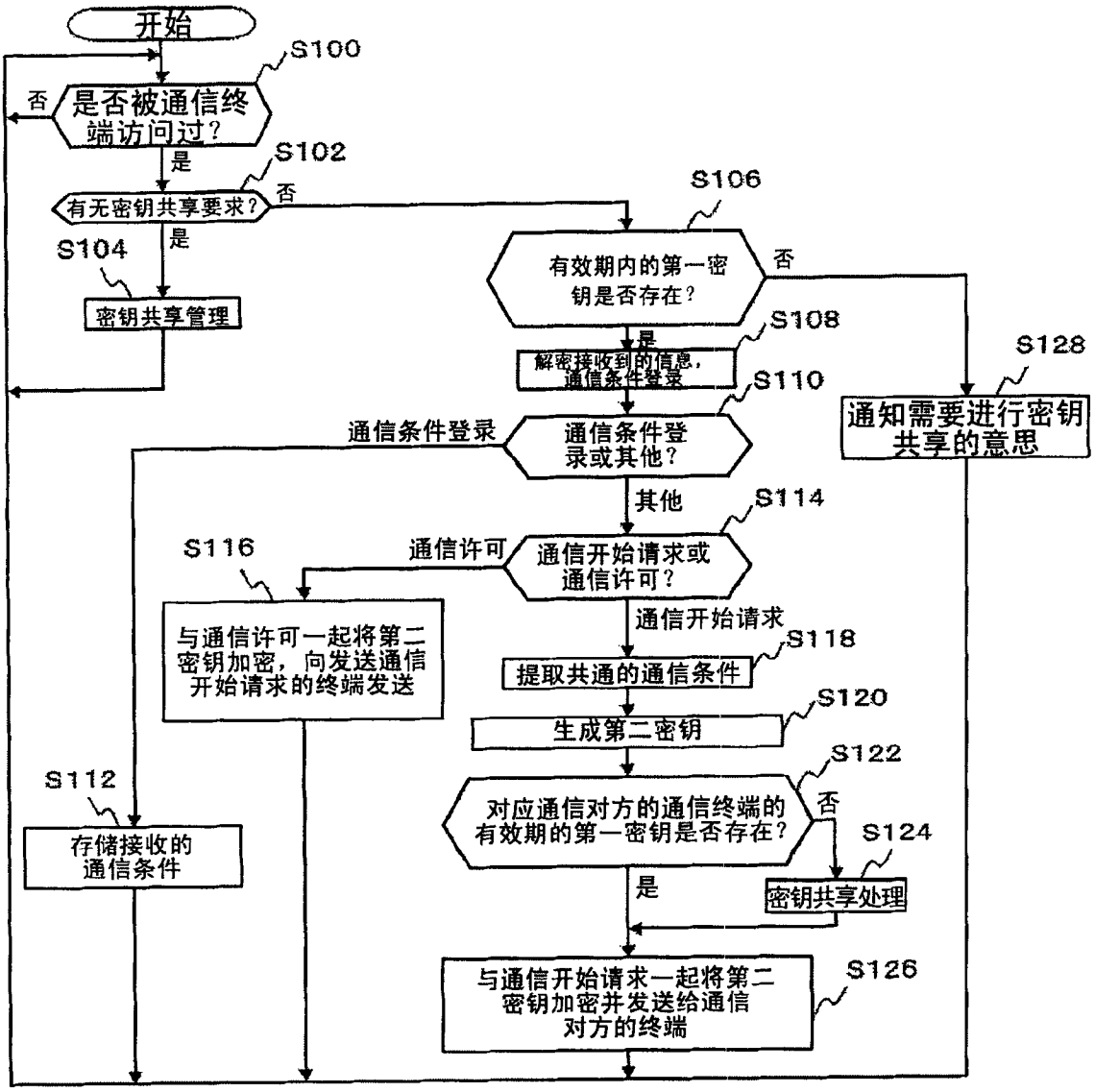

开始
S100
是否被通信终端访问过？
否
是
S102
有无密钥共享要求？
否
是
S104
密钥共享管理
S106
有效期内的第一密钥是否存在？
否
是
S108
解密接收到的信息，通信条件登录
S110
通信条件登录
通信条件登录或其他？
其他
S114
通信许可
通信开始请求或通信许可？
S116
与通信许可一起将第二密钥加密，向发送通信开始请求的终端发送
通信开始请求
S118
提取共通的通信条件
S120
生成第二密钥
S122
对应通信对方的通信终端的有效期的第一密钥是否存在？
否
是
S124
密钥共享处理
S126
与通信开始请求一起将第二密钥加密并发送给通信对方的终端
S112
存储接收的通信条件
S128
通知需要进行密钥共享的意思

图 9

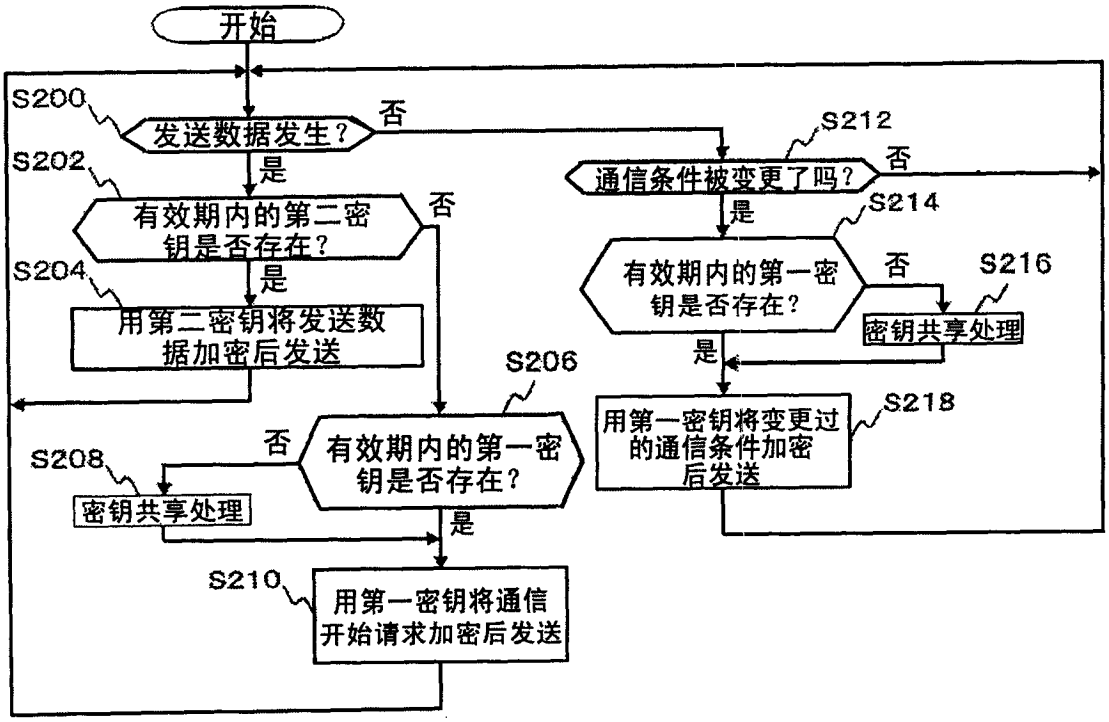

开始
S200
发送数据发生？
否
是
S202
有效期内的第二密钥是否存在？
否
是
S204
用第二密钥将发送数据加密后发送
S206
有效期内的第一密钥是否存在？
否
是
S208
密钥共享处理
S210
用第一密钥将通信开始请求加密后发送
S212
通信条件被变更了吗？
否
是
S214
有效期内的第一密钥是否存在？
否
是
S216
密钥共享处理
S218
用第一密钥将变更过的通信条件加密后发送

图 10

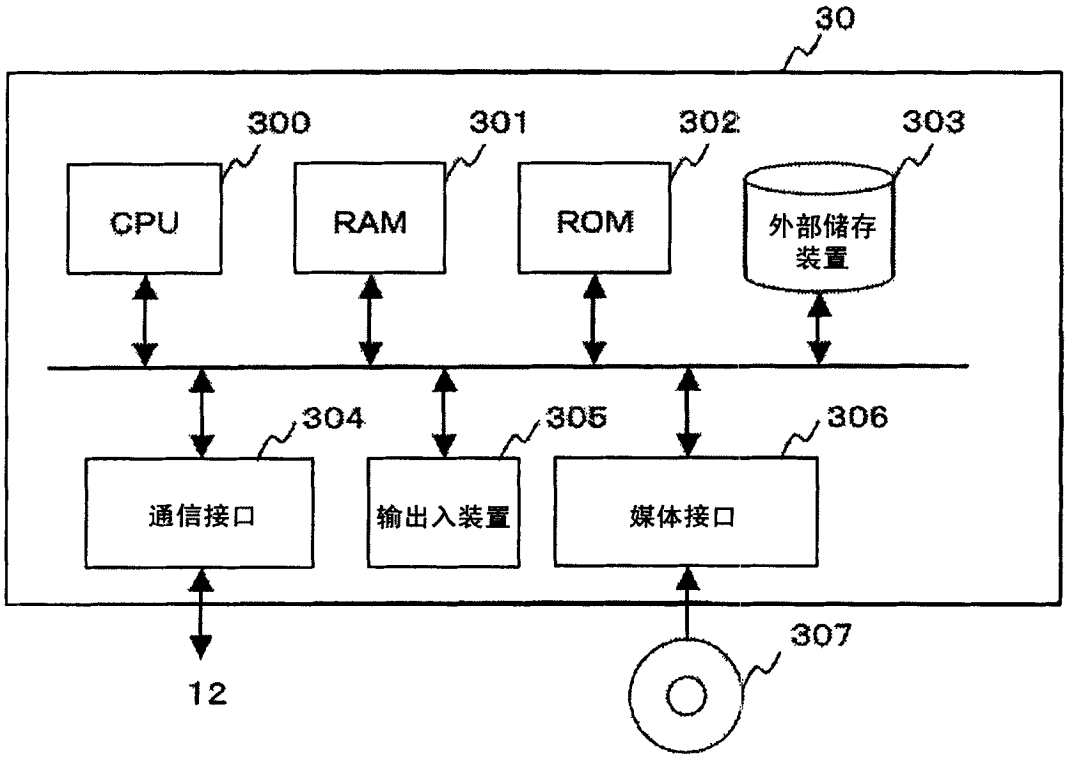

30
300
CPU
301
RAM
302
ROM
303
外部储存装置
304
通信接口
305
输出入装置
306
媒体接口
307
12

图 13

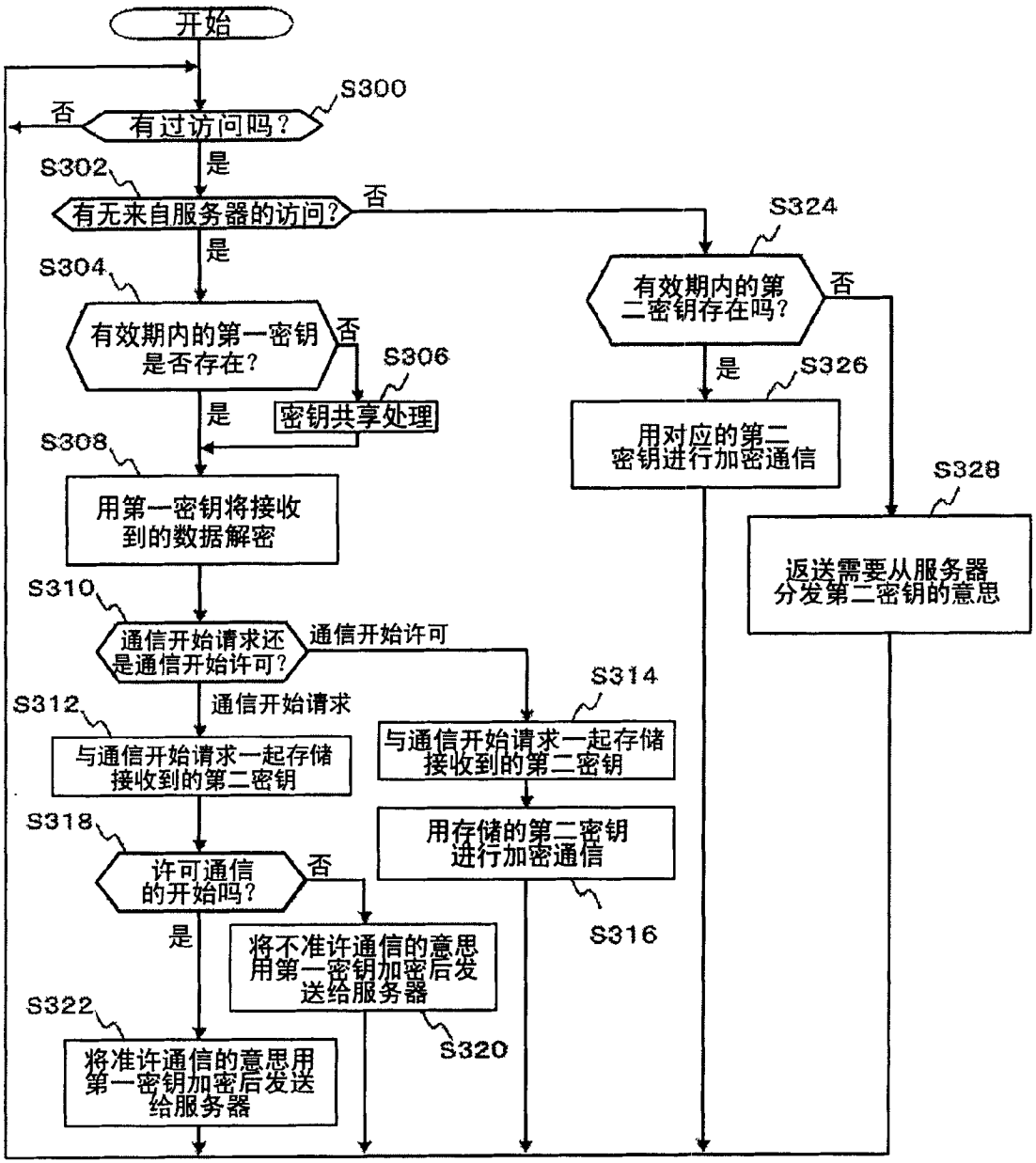

开始
S300
有过访问吗?
否
是
S302
有无来自服务器的访问?
否
是
S304
有效期内的第一密钥是否存在?
否
S306
密钥共享处理
是
S308
用第一密钥将接收到的数据解密
S310
通信开始请求还是通信开始许可?
通信开始许可
通信开始请求
S312
与通信开始请求一起存储接收到的第二密钥
S318
许可通信的开始吗?
否
是
S322
将准许通信的意思用第一密钥加密后发送给服务器
将不准许通信的意思用第一密钥加密后发送给服务器
S320
S314
与通信开始请求一起存储接收到的第二密钥
用存储的第二密钥进行加密通信
S316
S324
有效期内的第二密钥存在吗?
否
是
S326
用对应的第二密钥进行加密通信
S328
返送需要从服务器分发第二密钥的意思

图 11

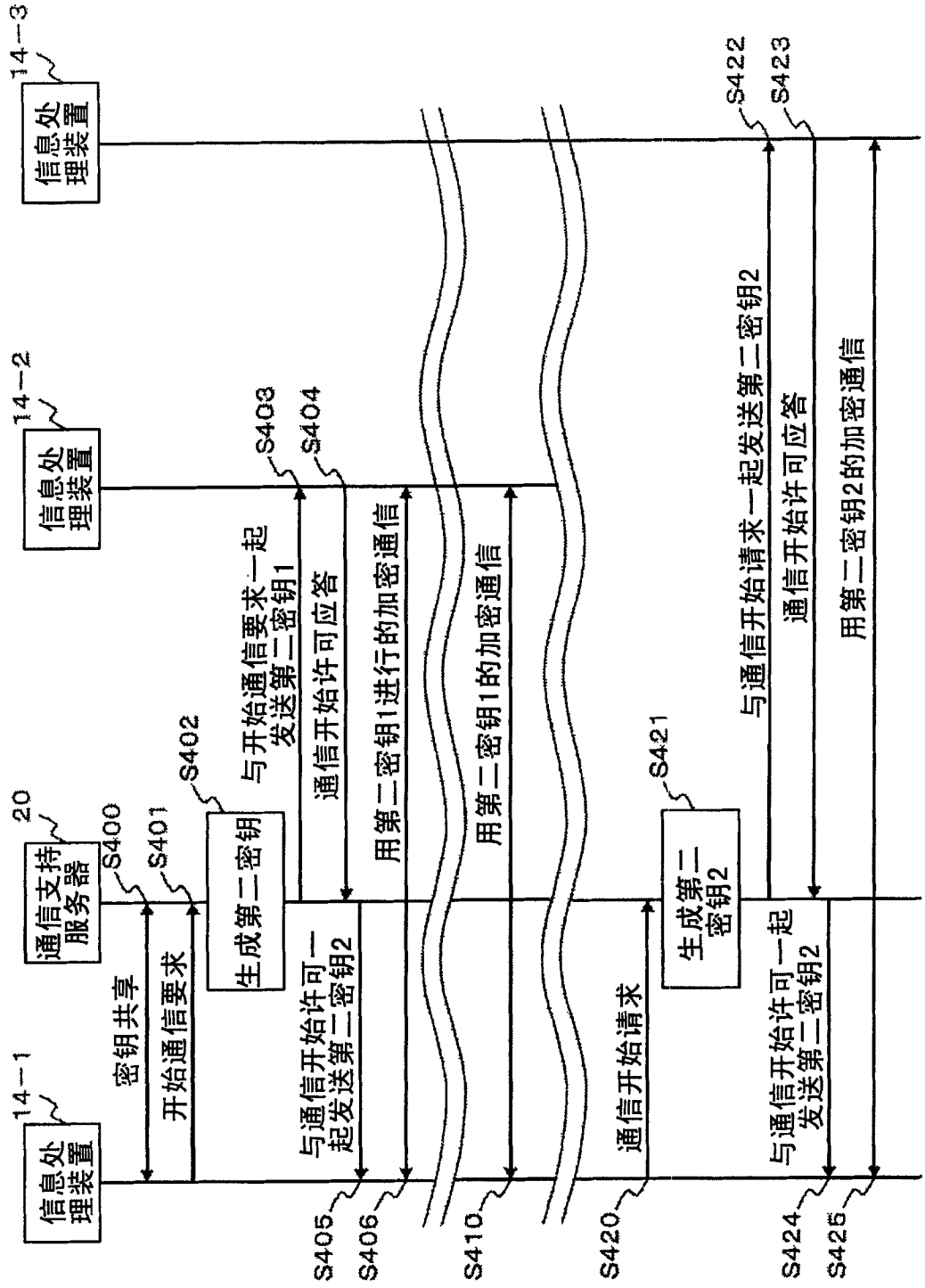

14-1
信息处理装置
20
通信支持服务器
14-2
信息处理装置
14-3
信息处理装置
密钥共享
开始通信要求
S400
S401
S402
生成第二密钥
与开始通信要求一起发送第二密钥1
S403
通信开始许可应答
S404
与通信开始许可一起发送第二密钥2
用第二密钥1进行的加密通信
S405
S406
用第二密钥1的加密通信
S410
通信开始请求
S420
S421
生成第二密钥2
与通信开始请求一起发送第二密钥2
S422
通信开始许可应答
S423
与通信开始许可一起发送第二密钥2
S424
用第二密钥2的加密通信
S425

图 12