(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 1783778 B
(45)授权公告日 2011.03.30

(21)申请号 200510125751.7

(22)申请日 2005.12.01

(30)优先权数据
2004-350099 2004.12.02 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 竹岛由晃 小川贵央

(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 9/14(2006.01)
H04L 12/66(2006.01)

(56)对比文件
CN 1358386 A,2002.07.10, 说明书第5页第20行至第8页第20行、图2-4.
US 2002/0007415 A1,2002.01.17, 全文.
US 2003/0131259 A1,2003.07.10, 说明书第0031-0033,0036段、图2-3.

审查员 刘玲斐

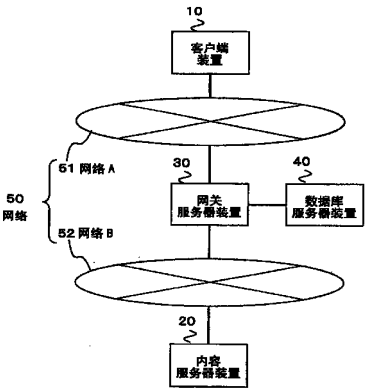
权利要求书 3 页 说明书 16 页 附图 12 页

(54)发明名称

网关服务器、及加密通信的中继方法

(57)摘要

无须对客户端装置追加特殊的功能，在网关服务器装置中就能够进行对End-End加密通信的附加价值处理，从而实现灵活的加密通信的中继方法。网关服务器装置30，生成暂时的加密通信许可证和与其成对的秘密密钥，使用它们在客户端装置10与网关服务器装置30之间进行加密通信。届时，把加密通信中继许可证、秘密密钥、客户端装置10的IP地址、内容服务器名、通信方法等登录在数据库服务器装置40内。然后，在与内容服务器装置20之间进行加密通信。因此，在网关服务器装置30中，由于暂时终止加密通信，所以在此就能够进行种种附加价值处理。



CN 1783778 B

1. 一种网关服务器装置中的加密通信的中继方法，其特征在于：

该方法，是中继在受理利用者的内容信息的访问请求并将根据该访问请求的访问请求消息向网络发送的客户端装置与接收从所述客户端装置经所述网络发送的所述访问请求消息并向所述客户端装置发送表示所述访问请求消息的内容信息的内容服务器装置之间、进行的加密通信的网关服务器装置中的加密通信的中继方法；

所述网关服务器装置，

具备：数据库，该数据库登录暂时的加密通信中继许可证、与其成对的秘密密钥、其有效期限、加密通信连接消息内的目的地服务器名、发送源客户端装置的 IP 地址、加密通信方法名；

执行如下步骤：

从所述客户端装置接收向所述内容服务器装置的加密通信连接消息的第一步骤；

第七步骤，该步骤，以包含在所述加密通信连接消息内的目的地服务器名、发送源客户端装置的 IP 地址之任一个或其两方为检索关键字，检索所述数据库，其结果，在适合于所述检索关键字的登录信息存在并且包含在该登录信息内的有效期限是在有效期限内的情况下，从所述登录信息中读出对所述目的地服务器名的内容服务器装置的暂时的加密通信中继许可证和与其成对的秘密密钥，不存在适合于所述检索关键字的登录信息的情况下、或者即使存在适合于所述检索关键字的登录信息而包含在该登录信息内的有效期限已经期满的情况下，生成针对包含在所述加密通信连接消息内的目的地服务器名的内容服务器装置的暂时的加密通信中继许可证和与其成对的秘密密钥，并把所述生成的暂时的加密通信中继许可证和与其成对的秘密密钥、其有效期限、所述加密通信连接消息内的目的地服务器名、发送源客户端装置的 IP 地址、加密通信方法名登录在所述数据库中；

把所述暂时的加密通信中继许可证发送到所述客户端装置的第三步骤；

在与所述客户端装置之间进行端到端加密通信，接收该客户端装置发送 的被加过密的访问请求消息，并把该加过密的访问请求消息解密后变换成明文的访问请求消息的第四步骤；

根据所述明文的访问请求消息的内容，与内容服务器装置进行端到端加密通信，并取得所述访问请求消息指示的内容信息的第五步骤；和

对所述取得的内容信息及其通信头进行附加价值处理，并把该附加价值处理后的所述内容信息及其通信头加密后发送到所述客户端装置的第六步骤。

2. 如权利要求 1 所述的加密通信的中继方法，其特征在于：

所述数据库，是被构成在与所述网关服务器装置不同的其他信息处理装置上的数据库。

3. 如权利要求 1 或 2 所述的加密通信的中继方法，其特征在于：

所述网关服务器装置，在执行所述第一步骤之后，还执行第八步骤，该步骤，把同意确认显示信息发送到所述客户端装置，该同意确认显示信息，是用来获得所述客户端装置的利用者对将从所述客户端装置发送的加过密的访问请求消息解密后变换为明文的访问请求消息的同意的信息，在从所述客户端装置接收到意味着所述利用者的同意确认的访问请求的情况下，把用来验证所述加密通信中继许可证的根认证局证书发送到所述客户端装置。

4. 如权利要求 1 或 2 所述的加密通信的中继方法，其特征在于：

当所述内容服务器装置进行客户端认证时，所述第五步骤还包括：将客户端装置编组并发送对应于该组而生成的客户端代理证书，而不由客户端装置发送客户端证书。

5. 一种网关服务器装置，其特征在于：

该网关服务器装置，中继在受理利用者的内容信息的访问请求并将根据该访问请求的访问请求消息向网络发送的客户端装置与接收从所述客户端装置经所述网络发送的所述访问请求消息并向所述客户端装置发送表示所述访问请求消息的内容信息的内容服务器装置之间、进行的加密通信；

所述网关服务器装置，

具备：数据库，该数据库登录暂时的加密通信中继许可证、与其成对的秘密密钥、其有效期限、加密通信连接消息内的目的地服务器名、发送源客 户端装置的 IP 地址、加密通信方法名；

具备下述单元：

从所述客户端装置接收向所述内容服务器装置的加密通信连接消息的第一单元；

第七单元，该单元，以包含在所述加密通信连接消息内的目的地服务器名、发送源客户端装置的 IP 地址之任一个或其两方为检索关键字，检索所述数据库，其结果，在适合于所述检索关键字的登录信息存在并且包含在该登录信息内的有效期限是在有效期限内的情况下，从所述登录信息中读出针对所述目的地服务器名的内容服务器装置的暂时的加密通信中继许可证和与其成对的秘密密钥，不存在适合于所述检索关键字的登录信息的情况下或者即使存在适合于所述检索关键字的登录信息而包含在该登录信息内的有效期限已经期满的情况下，生成针对包含在所述加密通信连接消息内的目的地服务器名的内容服务器装置的暂时的加密通信中继许可证和与其成对的秘密密钥，并把所述生成的暂时的加密通信中继许可证、与其成对的秘密密钥、其有效期限、所述加密通信连接消息内的目的地服务器名、发送源客户端装置的 IP 地址、加密通信方法名登录在所述数据库中；

把所述暂时的加密通信中继许可证发送到所述客户端装置的第三单元；

在与所述客户端装置之间进行端到端加密通信，接收该客户端装置发送的加过密的访问请求消息，并把该加过密的访问请求消息解密后变换成明文的访问请求消息的第四单元；

根据所述明文的访问请求消息的内容，与内容服务器装置进行端到端加密通信，并取得所述访问请求消息指示的内容信息的第五单元；和

对所述取得的内容信息及其通信头进行附加价值处理，并把该附加价值处理后的所述内容信息及其通信头加密后发送到所述客户端装置的第六单元。

6. 如权利要求 5 所述的网关服务器装置，其特征在于：

所述数据库，是被构成在与所述网关服务器装置不同的其他信息处理装置上的数据库。

7. 如权利要求 5 或 6 所述的网关服务器装置，其特征在于：

所述网关服务器装置，还具备第八单元，该第八单元，把同意确认显示信息发送到所述客户端装置，该同意确认显示信息，是用来获得所述客户端装置的利用者对从所述客户端装置发送的加过密的访问请求消息解密后变换为明文的访问请求消息的同意的信息，在从

所述客户端装置接收到意味着所述利用者的同意确认的访问请求的情况下，把用来验证所述加密通信中继许可证的根认证局证书发送到所述客户端装置。

8. 如权利要求 5 或 6 所述的网关服务器装置，其特征在于：

当所述内容服务器装置进行客户端认证时，所述第五单元，将客户端装置编组并发送对应于该组而生成的客户端代理证书，而不由客户端装置发送客户端证书。

网关服务器、及加密通信的中继方法

技术领域

[0001] 本发明涉及加密通信的中继方法、中继加密通信的网关服务器装置、加密通信程序及加密通信程序的存储媒体。

[0002] 背景技术

[0003] 以因特网为代表的网络，就流经该网络的数据而言，未必是安全的，存在各种各样的危险性。其一是盗听。例如，存有恶意的人，只要用特殊的软件或硬件，盗听流经该网络的信息，这样就能够非法取得如在线购物时发送的他人的信用卡号等个人信息。另外，还存在服务器的冒充问题。第三者冒充已有的在线商店并准备假的订购页，如果利用者不意识到是假商店而输入信用卡号等个人信息，就被非法得到信用卡号。

[0004] 作为用来解决这样的盗听或冒充服务器问题，实现安全通信的技术，有基于SSL(Secure Socket Layer) 或作为其后继技术的 TLS(Transport LayerSecurity) 的加密通信。按照这些加密通信方法，例如进行加密通信的 Web 服务器和 Web 浏览器，首先在其间进行秘密密钥的交换等信号交换，然后按加密过的通信进行其后的通信。因此，网络的途中存在的中继装置等中，不能将其通信内容解密。这样，就能够防止第三者的盗听。

[0005] 可是，如上的仅仅发送者和接收者可解读的加密通信（下称 End-End 加密通信）能确保被通信的信息的安全，但还会发生以下说明的问题。

[0006] 网关服务器装置，与内部网和因特网连接，同时，又是中继其间的通信的中继装置。而且，具备监视是否从内部网向因特网未流出例如企业的秘密文档等或者是否从因特网向内部网未流入病毒或其它有害的信息等的功能。另外，网关服务器装置，还具备进行内部网与因特网之间的通信数据的格式变换等服务功能。这样的通信数据的监视或格式变换等，常常被叫做附加价值处理，并作为网关服务器装置的功能的一部分而固定下来。在提供因特网连接服务的 ISP（因特网服务提供商）中，这样的附加价值处理，是作为商业 性服务来进行。

[0007] 但是，网关服务器装置，不能对 SSL 等 End-End 加密通信提供这样的附加值处理的服务。即使是网关服务器装置或 ISP 服务器，也不能解读 End-End 加密通信中的密码，而无法知道其通信内容。因此，网关服务器装置不能切断存有恶意的第三者用 SSL 加密通信发送的病毒或其它有害的信息，也不能阻止用 SSL 加密通信使秘密文档流出到内部网之外。

[0008] 作为解决该问题的软件产品，WebWasher 公司正在用叫做 SSL 扫描器的名称来销售这种软件产品。按照其小册子（参照非专利文献 1），SSL 扫描器被安装在网关服务器装置等内，来监视 Web 服务器（内容服务器装置）和 Web 客户端（客户端装置的浏览器）之间的 SSL 加密通信，这是进行加密数据的解密的通信中继软件。即，SSL 扫描器把 SSL 加密通信的加密文暂时变换为明文，就可以作为明文施加病毒检查等附加价值处理。

[0009] 在非专利文献 1 中，虽然未详细说明 SSL 扫描器可以挤入 SSL 加密通信的途中的方法或手段，但是可推测基于如下的方法的方法或手段。首先，SSL 扫描器的运用管理者向用户发布 SSL 扫描器的根 CA(Certificate Authority 证明管理机构）证书，并把该证书安装在浏览器中。而后，在浏览器与 Web 服务器之间进行 SSL 加密通信时之际，SSL 信号交换

时，SSL 扫描器把服务器证书发送给浏览器，由此，在 SSL 扫描器与浏览器之间进行 SSL 加密通信。

[0010] 在网关服务器装置中把加密通信文解密，然后对解了密的明文的通信文进行附加价值处理的例子，也存在于使用移动电话等的移动体通信中。把移动体的数据通信方法标准化的标准化团体 OMA(Open Mobile Allience 开放移动联盟)，在 WAP(Wireless Application Protocol 无线应用协议）版本 1 中规定了可进行 WAP 浏览器和网关服务器装置之间的加密通信的 WTLS(Wireless Transport Layer Security 无线传输层安全性）技术标准（参照非专利文献 2)。按照该 WAP 版本 1，移动电话等移动体终端上的 WAP 浏览器，在移动电话等与连接因特网的网关服务器装置之间进行依据 WTLS 的加密通信，并在网关服务器装置与 Web(WAP) 服务器之间进行 SSL 加密通信。

[0011] 这种情况下，网关服务器装置，为了中继双方的加密通信文，要将各自的加密通信文暂时解密成明文。因此，网关服务器装置，能够对 WAP 标准的 加密通信文自由地进行附加价值处理。即使在现实中，在面向移动电话的系统内，网关服务器装置，也在进行通信中的 HTTP 头上附加特殊的头等附加价值处理。

[0012] 【非专利文献 1】“产品信息 Webwasher SSL Scanner”,[online],[平成 16 年 8 月 6 日检索],因特网 <http ://www.webwasher.jp/pro#sslscanner.html>

[0013] 【非专利文献 2】“Wireless Transport Layer Security”,[online],2001 年 4 月，Wireless Application Protocol Forum,Ltd,[平成 16 年 8 月 6 日检索],因特网

[0014] <http ://www.openmobilealliance.org/tech/affiliates/wap/wap-261-wtls-20010406-a.pdf>

[0015] 但是，SSL 扫描器，不指定正在进行 SSL 加密通信的内容服务器装置或客户终端，而将 SSL 加密通信文变换成明文，再根据需要进行附加价值处理。因此，在 SSL 扫描器中，不能对每个正在进行 SSL 加密通信的内容服务器装置或客户终端装置，变更该通信方法的设定或设定所进行的附加价值处理。另外，有这样的问题，即 WTLS 加密通信，不是一般普及的方法，所以必须把可进行 WTLS 加密通信的功能追加到客户终端装置的 WEB 浏览器内。

发明内容

[0016] 鉴于上述的现有技术的问题，本发明的目的在于提供这样一种网关服务器装置和加密通信的中继方法、程序以及程序存储媒体：即不在客户终端装置的 WEB 浏览器内追加特殊的功能，就能在网关服务器装置中，进行针对 End-End 加密通信的附加价值处理，而且，能够根据内容服务器装置和客户终端装置，变更该通信方法的设定，或设定执行的附加价值处理。

[0017] 为了实现上述目的，本发明的网关服务器装置中的加密通信的中继方法，是中继在受理利用者的内容信息的访问请求并将根据该访问请求的访问请求消息向网络发送的客户端装置与接收从所述客户端装置经所述网络发送的所述访问请求消息并向所述客户端装置发送表示所述访问请求消息的内容信息的内容服务器装置之间、进行的加密通信的网关服务器装置中的加密通信的中继方法；；其特征在于：该网关服务器装置，执行如下步骤：从客户端装置接收用来向内容服务器装置的加密通信的连接消息的第一步骤；生成针对包 含在该连接消息内的目的地服务器名的内容服务器装置的暂时的加密通信中继许可

证和与其成对的秘密密钥的第二步骤；把该暂时的加密通信中继许可证发送到客户端装置的第三步骤；在与客户端装置之间进行 End-End 加密通信、接收该客户端装置发送的加过密的访问请求消息、再把加过密的访问请求消息解密后变换成明文的访问请求消息的第四步骤；根据该明文的访问请求消息的内容与内容服务器装置进行 End-End 加密通信、并取得访问请求消息指示的内容信息的第五步骤；对该取得的内容信息及其通信头进行附加价值处理、然后把该附加价值处理后的内容信息及其通信头加密后发送到客户端装置的第六步骤。

[0018] 按照本发明，网关服务器装置，接收客户端装置向内容服务器装置发送的用于加密通信的连接消息，然后生成针对客户端装置的暂时的加密通信中继许可证和与其成对的秘密密钥，所以，在客户端装置与网关服务器装置之间能够进行 End-End 加密通信。另外，网关服务器装置，根据由客户端装置发送的对内容服务器装置的访问请求，进行与内容服务器装置之间的 End-End 加密通信，并可以取得客户端装置要求的内容方法。即，本发明中，在客户端装置与内容服务器装置之间进行的加密通信，暂时被客户端装置与网关服务器装置之间的加密通信终止。因此，在所终止的网关服务器装置中，由于加密通信的消息被明文化，所以能够对被明文化的消息进行种种附加价值处理。

[0019] 在本发明中，客户端装置与网关服务器装置之间，以及网关服务器装置与内容服务器装置之间的通信，分别按 End-End 加密通信来进行。因此，即使它们之间进行着网络连接，也可以保证信息的安全性。

[0020] 本发明的其他加密通信的中继方法，其特征在于：在前述的加密通信的中继方法中，网关服务器装置，具备登录暂时的加密通信中继许可证和与其成对的秘密密钥、其有效期限、包含在所述加密通信连接消息内的目的地服务器名、发送源客户端装置的 IP 地址、加密通信方法名之任一个或其全部的数据库；并取代第二步骤执行第七步骤，该第七步骤，以包含在所述加密通信连接消息内的目的地服务器名、发送源客户端装置的 IP 地址之任一个或其两方为检索关键字检索该数据库，其结果，在适合于所述检索关键字的登录 信息存在并且包含在该登录信息内的有效期限是在有效期限内的情况下，从该登录信息中读出对所述目的地服务器名的内容服务器装置的暂时的加密通信中继许可证和与其成对的秘密密钥，不存在适合于所述检索关键字的登录信息的情况下，或者即使存在适合于所述检索关键字的登录信息而包含在该登录信息内的有效期限已经期满的情况下，生成对包含在所述加密通信连接消息内的目的地服务器名的内容服务器装置的暂时的加密通信中继许可证和与其成对的秘密密钥，然后把所述生成的暂时的加密通信中继许可证和与其成对的秘密密钥、其有效期限、包含在所述加密通信连接消息内的目的地服务器名、发送源客户端装置的 IP 地址、加密通信方法名之任一个或其全部登录在数据库中。

[0021] 按照本发明，对于目的地服务器名、发送源客户端装置的 IP 地址之任一个或其对，将暂时的加密通信中继许可证和与其成对的秘密密钥、其有效期限和加密通信方法名登录在数据库内。只要利用该数据库，就能够对每个客户端装置、每个内容服务器或每个其两方设定加密通信方法或附加价值处理。因此，就能够进行灵活的加密通信的中继。

[0022] 无需对 WEB 客户端追加特殊的功能，就能够在网关服务器装置中进行对客户端装置与内容服务器装置之间的 End-End 加密通信的附加价值处理，并能够依据内容服务器装置和客户端装置，灵活地设定其间的通信方法或进行的附加价值处理，从而可实现灵活的

加密通信的中继。

附图说明

[0023] 图 1 是适用本发明的网络系统的构成示意图；

[0024] 图 2 是用于适用本发明的网络系统的信息处理装置的构成图；

[0025] 图 3 是本发明的第一实施方式的网关服务器装置和数据库服务器装置的构成图；

[0026] 图 4 是本发明的第一实施方式中网关服务器装置中继客户端装置与内容服务器装置之间的 SSL 加密通信的处理的流程图；

[0027] 图 5 是对图 4 中的加密通信设定数据库的服务器检索处理（步骤 S002）的详细流程图；

[0028] 图 6 是对图 4 中的加密通信设定数据库的服务器登录处理（步骤 S010）的详细流程图；

[0029] 图 7 是对图 4 中的加密通信设定数据库的服务器消除处理（步骤 S008）的详细流程图；

[0030] 图 8 是图 4 中的分割型 SSL 加密通信处理（步骤 S006）的详细流程图；

[0031] 图 9 是图 8 中的 SSL 加密通信处理（步骤 S415）的详细流程图；

[0032] 图 10 是图 8 中的错误处理（步骤 S109）的详细流程图；

[0033] 图 11 是图 8 中的高速缓存应答处理（步骤 S408）的详细流程图；

[0034] 图 12 是图 4 中的用户同意确认处理（步骤 S600）的详细流程图；

[0035] 图 13 是图 12 的用户同意确认处理中所使用的用户同意确认页的示例图；

[0036] 图 14 是本发明的第一实施方式中进行附加价值处理的示例图；

[0037] 图 15 是本发明的第二实施方式中把客户端编组后进行代理认证的情况下的 Split SSL 加密通信处理的流程示例图。

[0038] 【符号说明】

[0039] 10 客户端装置

[0040] 20 内容服务器装置

[0041] 30 网关服务器装置

[0042] 40 数据库服务器装置

[0043] 50 网络

[0044] 301HTTP 代理处理部

[0045] 302 认证局服务器部

[0046] 303 加密通信处理部

[0047] 304 密钥管理部

[0048] 401 加密通信设定数据库

[0049] 1000 信息处理装置

[0050] 1001CPU

[0051] 1002 存储器

[0052] 1003 可移动存储媒体读取装置

[0053] 1004 通信装置

[0054] 1005 辅助存储装置

[0055] 1006 输入输出装置

[0056] 1008 可移动存储媒体

[0057] 4011 服务器名字段

[0058] 4012 通信方法字段

[0059] 4013 客户端 IP 地址字段

[0060] 4014 有效期限字段

[0061] 4015 加密通信中继许可证字段

[0062] 4016 秘密密钥字段

具体实施方式

[0063] < 第一实施方式 >

[0064] 以下适当参照图 1 ～图 11 详细说明本发明的第一实施方式。

[0065] (网络系统的构成)

[0066] 图 1 是适用本发明的网络系统的构成示意图。图 1 中，客户端装置 10、内容服务器装置 20、网关服务器装置 30 和数据库服务器装置 40 分别由叫做所谓计算机的信息处理装置构成。

[0067] 客户端装置 10，是利用者使用的信息处理装置，受理由利用者提出的内容信息的访问请求，根据该访问请求经网络 50 把访问请求信息发送到内容服务器装置 20。内容服务器装置 20 是保管大量有用信息 (内容信息) 的信息处理装置，接收客户端装置 10 发送的访问请求信息，并将该访问请求消息表示的内容信息发送到客户端装置 10。

[0068] 客户端装置 10 经网络 A51、网关服务器装置 30、网络 B52 连接到内容服务器装置 20 上。这里，网络 A51，例如是像 LAN(局域网) 那样的内部网络，网络 B52 例如是作为公共网络的因特网。另外，本实施方式中，在无需区别网络 A51 和网络 B52 的情况下，简单地叫做网络 50。

[0069] 网关服务器装置 30 处于网络 A51 和网络 B52 之间，是中继其间进行的通信的信息处理装置。另外，数据库服务器装置 40，在本实施方式中例如是利用关系型数据库管理网关服务器装置 30 中继客户端装置 10 与内容服务器装置 20 之间的通信时必要的信息的信息处理装置。对网关服务器装置 30 和数据库服务器装置 40 另作详细说明。

[0070] 图 2 是用于适用本发明的网络系统的信息处理装置的构成图。图 2 中，信息处理装置 1000，包含 CPU(中央处理单元)1001、由 RAM(随机存取存储器) 等半导体存储器构成的存储器 1002、像 CD-ROM(光盘只读存储器) 驱动器那样的可移动存储媒体读取装置 1003、连接在网络 50 上的通信装置 1004、像硬盘磁存储装置那样的非挥发性大容量的辅助存储装置 1005 和键盘或鼠标器或显示器等输入输出装置。网络 50 物理上由使用同轴电缆或光缆、无线等的通信线路和集线器或路由器那样的网络装置构成。

[0071] 存储器 1002 中存储信息处理装置 1000 执行的程序。即，客户端装置 10、内容服务器装置 20、网关服务器装置 30 和数据库服务器装置 40，在各个信息处理装置 1000 中，用可移动存储媒体读取装置 1003 读取记录在 CD-ROM 等可移动存储媒体 1008 内的规定的程序，装入存储器 1002。而后，由 CPU1001 执行被装在存储器 1002 中的程序，由此来实现各装置

10、20、30、40 中所规定的功能。

[0072] 也可以由同样连接在网络 50 上的其他信息处理装置 1000 经网络 50 和通信装置 1004 来进行向存储器 1002 的程序的装载。作为存储器 1002 使用半导体非挥发性存储器，也可以预先把程序写入该半导体非挥发性存储器内。如果使用向该存储器 1002 的程序的装载装置，各装置 10、20、30、40 就不一定必须具备可移动存储媒体读取装置 1003 和辅助存储装置 1005。例如，客户端装置 10 也可以是移动电话那样的小型信息处理装置 1000。

[0073] 图 1 中，客户端装置 10 是执行 Web 浏览器等现有的 Web 客户端应用程序的信息处理装置 1000。即，客户端装置 10，例如是具备因特网通信功能的个人计算机、移动电话等。另外，内容服务器装置 20，是执行现有的种种服务器应用程序的信息处理装置 1000。例如，是提供文档・运动图像数据或程序文件等的 Web 服务器，或是提供其他 Web 服务的应用服务器等。

[0074] 这样的客户端装置 10 和内容服务器装置 20 中，客户端装置 10，首先，对内容服务器装置 20 发送要求内容服务器装置 20 存储的文档数据或运动图像数据、程序文件等内容的下载的通信消息（访问请求）。于是，内容服务器装置 20 对此作出应答，并把客户端装置 10 要求的内容发送到客户端装置 10。

[0075] 网关服务器装置 30 是进行通信消息的中继的装置，例如，可以用 Web 代理服务器来实现。网关服务器装置 30 把由客户端装置 10 经由网络 A51 发送来的通信消息中继到内容服务器装置 20。成为目的地的内容服务器装置 20 的信息（主机名或 IP 地址等），作为内容的 URL(Uniform Resouce Locator) 信息被包含在访问请求的通信消息中。另外，网关服务器装置 30，往往也具备作为高速缓存存储中继的应答内容的高速缓存功能。

[0076] 另外，数据库服务器装置 40，本实施方式中一并管理网关服务器装置 30 中继客户端装置 10 与内容服务器装置 20 之间的通信时必要的信息。数据库服务器装置 40，例如，可以用关系型数据库等来实现，可以处理来自多个网关服务器装置 30 的数据库检索要求、数据登录要求、数据消除要求等。

[0077] 物理上也可以用一个信息处理装置 1000 来实现在构成图 1 的网络系统的各装置 10、20、30、40 分别实现的功能。例如，数据库服务器装置 40 的功能也可以包含在网关服务器装置 30 内。另外，由一个装置实现的功能，物理上也可以用多个装置来实现。例如，也可以用经网络 50 与网关服务器装置 30 通信的其他信息处理装置 1000 来实现包含在网关服务器装置 30 内的功能的一部分。

[0078] （网关服务器装置和数据库服务器装置的构成）

[0079] 图 3 是本实施方式中的网关服务器装置和数据库服务器装置的构成图。图 3 中，网关服务器装置 30，由 HTTP(Hyper Text Transfer Protocol) 代理处理部 301、认证局服务器部 302、加密通信处理部 303、密钥管理部 304 构成。另外，数据库服务器装置 40 由加密通信设定数据库 401 构成。

[0080] HTTP 代理处理部 301，中继从客户端装置 10 向内容服务器装置 20 发送的访问请求。另外，在非加密通信中，进行高速缓存从客户端装置 10 向内容服务器装置 20 发送的应答数据等附加处理。

[0081] 认证局服务器部 302，对 HTTP 代理处理部 301 指示的服务器名的服务器，发行具有公开密钥证书的形式的暂时的加密通信中继许可证 40151 和生成与其成对的秘密密钥。

[0082] 加密通信处理部 303，经 HTTP 代理处理部 301 进行与客户端装置 10 或内容服务器装置 20 之间的 End-End 加密通信。另外，通过 End-End 加密通信进行从内容服务器装置 20 下载下来的内容的高速缓存。

[0083] 密钥管理部 304 保管根 CA 认证局发行的网关服务器装置 30 用的秘密密钥和公开密钥证书、用来验证内容服务器装置 20 的公开密钥证书的根认证局证书。

[0084] 图 3 中，数据库服务器装置 40 具备加密通信设定数据库 401。加密通信设定数据库 401，例如用关系型数据库来构建。网关服务器装置 30，对数据库服务器装置 40，用 SQL(Structured Query Language 结构查询语言）语言等数据库操作用语言来进行加密通信设定数据库 401 的检索、登录、消除等处理。

[0085] 加密通信设定数据库 401，被用来用表格形式的数据库管理加密通信的设定。按照每个内容服务器装置名和客户端 IP 地址来管理加密通信的设定信息。即，加密通信设定数据库 401，由服务器名字段 4011、通信方法字段 4012、客户端 IP 地址字段 4013、有效期限字段 4014、加密通信中继许可证字段 4015 和秘密密钥字段 4016 等构成。另外，加密通信设定数据库 401，以表目 4019 为单位来管理这些信息，也就是说，加密通信设定数据库 401 的检索、登录、消除等处理以表目 4019 为单进行处理。另外，有时也把表目叫做记录。

[0086] 以下详细说明加密通信设定数据库 401 的各字段 4011 ～ 4016。

[0087] 服务器名字段 4011 是管理连接在网络 B52 上的内容服务器装置 20 的主机名的字段。按照如“www.example.com”那样的 FQDN(Fully Qualified DomainName) 形式或如“192.168.1.1”那样的 IP 地址形式来存储主机名。

[0088] 通信方法字段 4012 是管理客户端装置 10 与内容服务器装置 20 之间的加密通信方法的字段。作为通信方法的例子，有客户端装置 10 与内容服务器装置 20 之间进行的通常的 SSL 加密通信（以下叫做“End-End SSL”方法）和分割型的 SSL 加密通信（以下叫做“Split SSL”方法），该分割型的 SSL 加密通信，是用网关服务器装置 30 分别终止与客户端装置 10 的 SSL 加密通信和与内容服务器装置 20 的 SSL 加密通信而将客户端装置 10 与内容服务器装置 20 之间的 SSL 加密通信分割后的 SSL 加密通信方法。即，在“Split SSL”中，客户端装置 10 与内容服务器装置 20 之间的 SSL 加密通信的加密通信数据，在网关服务器装置 30 内被暂时解密而复原成明文。

[0089] 作为加密通信，除 SSL 加密通信之外，也可以是 TLS 加密通信。

[0090] 客户端 IP 地址字段 4013 是管理客户端装置 10 的 IP 地址的字段。可是，根据网络 A51 的系统，在每次通信时客户端的 IP 地址可能有变动的情况，所以，在这种情况下，也可以不是管理客户端装置 10 的 IP 地址，而是用客户端装置 10 的认证信息（用户 ID 或电话号码等）库来管理。在图 3 的通信方法的设定例中，就其对服务器名为“A.com”和“B.com”的服务器的访问来说，与客户端装置 IP 地址无关、适用“End-End SSL”的通信方法；另外，对于服务器名为“C.com”的服务器来说，在客户端装置 IP 地址是“192.168.A”的情况下，适用“Split SSL”通信方法；对于服务器名为“D.com”的服务器来说，在客户端装置 IP 地址是“192.168.B”的情况下，适用“Split SSL”通信方法。

[0091] 有效期限字段 4014，是管理各表目 4019 的设定的有效期限信息的字段，对于在该有效期限字段 4014 中有有效期限数据的表目 4019 来说，设定有效期限的日期（还可以包含时刻），而对于没有有效期限数据的表目 4019，则设定“—（无有效期限）”。

[0092] 加密通信中继许可证字段 4015，是管理加密通信中继许可证 40151 的数据的字段，网关服务器装置 30，把加密通信中继许可证的数据登录在该加密通信中继许可证字段 4015 内。通过进行登录，在有多个网关服务器装置 30 的情况下，不管客户端装置 10 访问哪个网关服务器装置 30，只要满足客户端 IP 地址 4013 或目标服务器名 4011、有效期限 4014 等条件，就能够从加密通信设定数据库 401 内取出同样的加密通信中继许可证 40151，并应答客户端装置 10。

[0093] 秘密密钥字段 4016 是管理秘密密钥的数据的字段，网关服务器装置 30 把自身的秘密密钥数据登录在该秘密密钥字段 4016 内。通过进行登录，在有多个网关服务器装置 30 的情况下，不管客户端装置 10 访问哪个网关服务器装置 30，只要满足客户端 IP 地址 4013 或目标服务器名 4011、有效期限 4014 等条件，就能够从加密通信设定数据库 401 内取出同样的秘密密钥，并用于与客户端装置 10 的加密通信。

[0094] 通过检索加密通信设定数据库 401，就能够取得登录在以上各字段 4011 ～ 4016 内的数据。在该检索中，当把任意一字段的值作为检索关键字来 检索加密通信设定数据库 401 时，就能够得到符合条件的表目 4019 的信息。在图 3 的例中，网关服务器装置 30 对数据库服务器装置 40 用『服务器名＝“A.com”』这样的检索关键字发送查询语句时，数据库服务器装置 40，就在加密通信设定数据库 401 中检索服务器名字段 4011 内包含“A.com”的表目 4019。然后，数据库服务器装置 40，对网关服务器装置 30，应答诸如『通信方法＝“End-End SSL”、客户端 IP 地址＝“无限制”、有效期限＝“无”、加密通信中继许可证＝“无”、秘密密钥＝“无”』的表目 4019。另外，数据库服务器装置 40 应答的信息，也可以仅仅作为网关服务器装置 30 必要的字段信息，可以用查询语句的参数来指定必要的字段信息。

[0095] (SSL 加密通信中继处理)

[0096] 图 4 是网关服务器装置中继客户端装置与内容服务器装置之间的 SSL 加密通信的处理的流程图。该处理流程表示：网关服务器装置 30 确立了与客户端装置 10TCP(Transmission Control Protocol 发送控制协议) 连接之后，从客户端装置 10 接收 HTTP 的 CONNECT 方法，进行通常的终端间通信 (End-EndSSL 加密通信)，或由网关服务器装置 30 进行的分割型 SSL 通信 (Split-SSL 加密通信)，直到结束 CONNECT 方法的处理为止的状态迁移。

[0097] 图 4 中，首先，网关服务器装置 30 的 HTTP 代理处理部 301，从客户端装置 10，接收包含 HTTP 的 CONNECT 方法的访问请求 (步骤 S001)。所谓 CONNECT 方法，是指示网关服务器装置 30 对内容服务器装置 20 进行 SSL 加密通信用 TCP 连接的方法。网关服务器装置 30，一接收 CONNECT 方法就开始 CONNECT 接收处理。

[0098] 然后，网关服务器装置 30 的 HTTP 代理处理部 301，从 CONNECT 方法的访问请求消息中，提取出成为目的地的内容服务器装置 20 的服务器名或 IP 地址。例如，在接收到的 HTTP 的访问请求消息的最初的行 (请求行) 内有字符串“CONNECT www.example.com :443 HTTP/1.1”的情况下，提取出字符串“www.example.com”，作为服务器名对待。然后，把该服务器名或 IP 地址作为检索关键字，对数据库服务器装置 40 进行向其加密通信设定数据库 401(图 4 中简单地记载为 DB) 的服务器检索处理 (步骤 S002)。另外，对服务器检索处理，用图 5 将另作更详细说明。

[0099] 另外，按照客户端装置 10 的设定，客户端装置 10，往往不发送 CONNECT 方法，而最

初把目的地的内容服务器装置 20 的 IP 地址设定为目的地 IP 地址，然后发送 IP 数据包，进行 SSL 加密通信的信号交换。在网关服务器装置 30 接收到该 IP 数据包的情况下，网关服务器装置 30，检查包含在 IP 数据包内的 TCP 头之中的目的地端口号，如果该目的地端口号是表示 SSL 加密通信的端口号，如 443 号，就认为用 TCP 信号交换以后的数据包来进行 SSL 加密通信的信号交换。然后，HTTP 代理处理部 301，把 IP 头中的目的地 IP 地址，作为目的地的内容服务器装置 20 的 IP 地址对待，并使用该 IP 地址进行对数据库服务器装置 40 的服务器检索指示（步骤 S002）及其以后的处理。

[0100] 接下来，用数据库服务器装置 40 中的检索结果，来判断检索到的服务器是否已经被登录到了数据库服务器装置 40 内（步骤 S003）。其结果，在应答了服务器名字段 4011 内包含检索关键字的服务器信息的情况下（步骤 S003 中“是”），HTTP 代理处理部 301，判定为在加密通信设定数据库 401 内已经登录完毕。在未应答包含检索关键字的服务器信息的情况下（步骤 S003 中“否”），判定为是未登录的服务器。

[0101] 因此，在 CONNECT 方法的目的地的内容服务器装置 20 的服务器名登录完的情况下（步骤 S003 中“是”），HTTP 代理处理部 301，接着进行有效期限检查（步骤 S004）。即，网关服务器装置 30，由于用软件或硬件管理着当前的日期和时刻，所以将当前的日期和时刻与由检索结果得到的有效期限字段 4014 的值相比较。

[0102] 然后，该时间在有效期限内的情况下（步骤 S004 中“是”），HTTP 代理处理部 301，接着进行通信方法检查（步骤 S005）。例如，判定检索结果得到的通信方法字段 4012 的值是“Split SSL”方法，还是“End-End SSL”方法。

[0103] 如果该通信方法是“Split SSL”方法（步骤 S005 中“是”），HTTP 代理处理部 301，进行 Split SSL 加密通信处理（步骤 S006）。Split SSL 加密通信处理，是这样的处理，即在与客户端装置 10 的通信中，网关服务器装置 30 作为 SSL 服务器而动作，终止与客户端装置 10 的 SSL 加密通信，并且与内容服务器装置 20 之间进行新的 SSL 加密通信。

[0104] 然后，HTTP 代理处理部 301，一旦由内容服务器装置 20 或客户端装置 10 切断 TCP 连接，就结束 Split SSL 加密通信处理。或者，因超时等某种理由，HTTP 代理处理部 301，切断与客户端装置 10 的 TCP 连接和与内容服务器装置 20 的 TCP 连接，这样也可以主动结束 Split SSL 加密通信处理。然后，网关服务器装置 30 结束 CONNECT 接收处理。

[0105] 另一方面，在步骤 S005，通信方法是“End-End SSL”方法的情况下（步骤 S005 中“否”），HTTP 代理处理部 301 进行 End-End SSL 加密通信处理（步骤 S007）。End-End SSL 加密通信处理，是 HTTP 代理服务器中继 SSL 加密通信的通常的通信处理方法。具体地说，首先，网关服务器装置 30 从客户端装置 10 接收到 HTTP-CONNECT 方法时，对由 CONNECT 目标指定的内容服务器装置 20 进行 TCP 连接；然后，TCP 信号交换正常结束之后，把表示连接结束的消息发送到客户端装置 10。该消息，例如是在 HTTP 应答的最初行（状态行）内记述为“HTTP/1.1 200 Connection establihed”的消息。此后，把从客户端装置 10 或内容服务器装置 20 发送的应用数据，传送到内容服务器装置 20 或客户端装置 10。另外，，HTTP 代理处理部 301 根据 TCP 连接，对 TCP 头或 IP 头等、应用数据以外的部分适宜地进行变换。

[0106] 然后，HTTP 代理处理部 301，一旦由内容服务器装置 20 或客户端装置 10 切断 TCP 连接，就结束 End-End SSL 加密通信处理。或者，因超时等某种理由，HTTP 代理处理部 301，主动切断与客户端装置 10 的 TCP 连接和与内容服务器装置 20 的 TCP 连接，这样，也可以结

束 End-End SSL 加密通信处理。然后，网关服务器装置 30 结束 CONNECT 接收处理。

[0107] 另外，在步骤 S004 中，在超过了有效期限的情况下（步骤 S004 中“否”），HTTP 代理处理部 301，对数据库服务器装置 40，进行加密通信设定数据库 401 的相应表目 4019 的消除处理（步骤 S008）。

[0108] 然后，检查在网关服务器装置 30 的设定之中，内容服务器装置 20 的信息未登录在加密通信设定数据库 401 内的情况下的 SSL 加密通信处理的缺省设定（步骤 S009），结果，在缺省设定是 End-End SSL 加密通信处理的情况下（步骤 S009 中“否”），进行步骤 S007 的处理。

[0109] 另一方面，在缺省设定是 Split SSL 加密通信处理（步骤 S009 中“否”）的情况下，对加密通信设定数据库 401 进行内容服务器装置 20 的信息的登录 处理（步骤 S010）。然后，在登录处理正常结束了的情况下（步骤 S011 中“否”），进行用户同意确认处理（步骤 S600）。关于用户同意确认处理另作详细说明。另外，在登录处理异常结束了的情况下（步骤 S011 中“是”），HTTP 代理处理部 301，主动切断与客户端装置 10 的 TCP 连接，由此，来结束 CONNECT 接收处理。

[0110] 另外，在步骤 S003，在 CONNECT 方法的目的地的内容服务器装置 20 的服务器名是未登录的情况下（步骤 S003 中“否”），HTTP 代理处理部 301，进行步骤 S009 以下的处理。

[0111] 图 5 是对图 4 中的加密通信设定数据库的服务器检索处理（步骤 S002）的详细流程图。

[0112] 图 5 中，网关服务器装置 30 的 HTTP 代理处理部 301（参照图 3），首先对数据库服务器装置 40，以 CONNECT 目标服务器名和客户端 IP 地址为检索关键字发行查询请求（步骤 S102）。将查询请求例如以 SQL 语言的形式转交给数据库服务器装置 40。于是，数据库服务器装置 40，解释该查询请求，并把与 CONNECT 目标服务器名相同的值存储在加密通信设定数据库 401 的服务器名字段 4011 内，而且查找在客户端 IP 地址字段 4013 内存储着与客户端 IP 地址同值的表目 4019。而后，如果有该表目 4019，就把该表目 4019 应答给 HTTP 代理处理部 301（步骤 S103），如果没有该表目 4019，就应答为检索无结果。检索结果的应答，至少包含通信方法字段 4012 的值、表目 4019 自身的有效期限字段 4014 的值、加密通信中继许可证 40151、与加密通信中继许可证 40151 成对的秘密密钥 40161。

[0113] 图 6 是对图 4 中的加密通信设定数据库的服务器登录处理（步骤 S010）的详细流程图。

[0114] 图 6 中网关服务器装置 30，首先生成对 CONNECT 目标服务器名的加密通信中继许可证 40151（步骤 S201），加密通信中继许可证 40151 是用来进行 End-End 加密通信的服务器公开密钥证书。服务器公开密钥证书，基于例如国际电信联合电信标准化部门（International Telecommunication Union-Telecommunication sector：ITU-T）劝告的 X.509 标准。并且，其中包含有证书的发行者或主体者（所有者）、有效期限、公开密钥信息和验证该证书的有效 性所必要的发行者的电子署名等信息。

[0115] 一般，认证局（Certification Authority：CA）对内容服务器装置 20 的运营者等发行服务器公开密钥证书。用户在下载了服务器公开密钥证书时，使用服务器公开密钥证书中的 CA 电子署名和用户预先保持着的 CA 公开密钥证书进行服务器公开密钥证书的验证，。这里，把用户信赖的 CA 称之为根 CA。用户把根 CA 的公开密钥证书安装在客户端装置

10 的浏览器等内，由此，就能够进行根 CA 或根 CA 信赖的其他 CA 发行的公开密钥证书的验证。

[0116] 在下载了根 CA 不信赖的 CA 发行的公开密钥证书的情况下，客户端装置 10 的浏览器会发出警告消息通知用户。网关服务器装置 30 的认证局服务器部 302 在 CONNECT 消息接收时每次发行加密通信中继许可证 40151 和与其成对的秘密密钥 40161。加密通信中继许可证 40151 的主体者是 CONNECT 目标内容服务器装置 20 名，发行者是网关服务器装置 30。

[0117] 然后，HTTP 代理处理部 301 对数据库服务器装置 40 进行表目追加请求（步骤 S202），追加的信息是 CONNECT 目标内容服务器装置 20 名、通信方法、客户端 IP 地址、有效期限、加密通信中继许可证 40151、秘密密钥 40161 等。通信方法，例如是“Split SSL”方法；有效期限，例如是根据预先设定在网关服务器装置 30 内的参数以把参数值追加到当前时刻上的日期和时刻进行设定。例如，CONNECT 消息接收时间是『2003 年 7 月 15 日 12:00:00』，如果参数值是『1 日』，有效期限就设定为『2003 年 7 月 16 日 12:00:00』。

[0118] 然后，数据库服务器装置 40 向 HTTP 代理处理部 301 应答登录处理结果（步骤 S203）。

[0119] HTTP 代理处理部 301 判定该应答结果（步骤 S204）；如果登录处理没问题地结束了，就结束登录处理（步骤 S204 中“是”）；如果登录处理失败，就异常结束（步骤 S204 中“否”）。

[0120] 图 7 是对图 4 中的加密通信设定数据库的服务器消除处理（步骤 S008）的详细流程图。

[0121] HTTP 代理处理部 301（参照图 3），首先对数据库服务器装置 40 进行加密通信设定数据库 401 的表目消除的请求（步骤 S301）。要消除的表目 4019，例如是以 CONNECT 目标内容服务器装置名和客户端 IP 地址为检索关键字而 满足检索条件的表目 4019。

[0122] 然后，数据库服务器装置 40，向 HTTP 代理处理部 301 应答消除处理结果（步骤 S302），HTTP 代理处理部 301 接收应答结果，结束消除处理。

[0123] 图 8 是图 4 中的 Split SSL 加密通信处理（步骤 S006）的详细流程图。

[0124] HTTP 代理处理部 301（参照图 3），一开始 Split SSL 加密通信处理，就把加密通信处理部 303 作为 CONNECT 目标的 SSL 服务器进行处理，具体地说，HTTP 代理处理部 301，把在步骤 S103 得到的加密通信中继许可证 40151 和秘密密钥 40161 转交给加密通信处理部 303。然后，HTTP 代理处理部 301，把从客户端装置 10 接收到的数据，暂时写入到存储器 1002 内。而后，加密通信处理部 303 从存储器 1002 读出该数据。然后通过进行其相反的处理，在客户端装置 10 与加密通信处理部 303 之间进行数据交接。

[0125] 另外，在加密通信处理部 303 在与 HTTP 代理处理部 301 不同的信息处理装置 1000 上动作的情况下，HTTP 代理处理部 301 与加密通信处理部 303，经网络 50 进行通信，进行数据的交接。HTTP 代理处理部 301，把从加密通信处理部 303 交接的数据，原样发送到客户端装置 10，或者追加或消除客户端装置 10 与 HTTP 代理处理部 301 的通信用的 HTTP 头后发送到客户端装置 10。另外，同样，HTTP 代理处理部 301 把从客户端装置 10 接收到的数据交接到加密通信处理部 303。

[0126] 然后，加密通信处理部 303，对客户端装置 10 发送针对 CONNECT 方法的应答后进行 SSL 信号交换处理（步骤 S402 ～ S405）。在步骤 S404，把服务器公开密钥证书发送到客户

端装置 10 时，取代内容服务器装置 20 的服务器公开密钥证书，由代理发送加密通信中继许可证 40151。

[0127] 接下来，加密通信处理部 303 从客户端装置 10 接收完成了加密的访问请求，并进行解密（步骤 S406）。这里，加密通信处理部 303，解析 CONNECT 目标内容服务器装置 20 的服务器名和所接收到的访问请求内的 URL，检查访问请求目标的内容是否全都被高速缓存了，而后，在被高速缓存了的情况下检查是否是在高速缓存的有效期限内（步骤 S407）。在保持着有效期限内的高速缓存的情况下（步骤 S407 中“是”），进行高速缓存应答处理（步骤 S408），结束 Split SSL 加密通信。

[0128] 另外，在步骤 S407，没有高速缓存或即使有有效期限已期满的情况下（步骤 S407 中“否”），加密通信处理部 303 对 CONNECT 目标内容服务器装置 20 进行 SSL 信号交换处理（步骤 S410 ～ S412）。这里，加密通信处理部 303 在进行与内容服务器装置 20 的 HTTP 连接时，对 HTTP 代理处理部 301 发送 CONNECT 方法，HTTP 代理处理部 301 解析 CONNECT 目标内容服务器装置 20 名后进行与相应的内容服务器装置 20 的 TCP 连接和 SSL 信号交换处理，这样，也可以经由 HTTP 代理处理部 301 进行与内容服务器装置 20 的通信。另外，加密通信处理部 303 也可以与内容服务器装置 20 进行直接 TCP 连接和 SSL 信号交换处理。然后，加密通信处理部 303，判定 SSL 信号交换处理结果是 SSL 信号交换成功还是失败（步骤 S413）。

[0129] 此后，在 SSL 信号交换处理成功的情况下（步骤 S413 中“是”），进行服务器公开密钥证书的验证（步骤 S414）；在该验证成功的情况下（步骤 S414 中“是”），进行 SSL 加密通信中继处理（步骤 S415）；此后，结束 Split SSL 加密通信处理。在步骤 S413SSL 信号交换处理失败的情况下，或者，在步骤 S414，公开密钥证书的验证失败的情况下，进行错误处理（步骤 S109），并结束 Split SSL 加密通信处理。

[0130] 图 9 是图 8 中的 SSL 加密通信处理（步骤 S415）的详细流程图。

[0131] 加密通信处理部 303（参照图 3），首先用在步骤 S410 ～ S412 确立的 SSL 连接对 CONNECT 目标的内容服务器装置 20 加密发送向访问请求目标的 URL 的访问请求（步骤 S501）；于是，内容服务器装置 20 把对该访问请求的应答数据加密之后发送到加密通信处理部 303（步骤 S502）。

[0132] 加密通信处理部 303，进行接收到的数据的解密处理（步骤 S503），对该数据进行数据格式的变换或高速缓存作成等附加价值处理（步骤 S504）。这里，作为附加价值处理的例子，除此之外，还有 HTTP 头或内容数据的追加或修正或消除等处理、步骤 S109 的 HTTP 错误处理或者按照分析内容数据的结果的与其他服务器的通信处理等。另外，用图 14 来补充说明附加价值处理的例子。

[0133] 然后，加密通信处理部 303，再次把与客户端装置 10 的 SSL 加密通信用数据加密（步骤 S505），然后发送到客户端装置 10（步骤 S506）；结束 SSL 加密通信中继处理。或者，在步骤 S506 之后，再次接收到与步骤 S406 同样的加密访问请求的情况下，也可以重复进行步骤 S406 以后的处理。另外，这种情况下，也可以设置限制时间，如果超过限制时间就结束 SSL 中继处理。

[0134] 图 10 是图 8 中的错误处理（步骤 S109）的详细流程图。

[0135] 在网关服务器装置 30（参照图 3）的 HTTP 代理处理部 301 或加密通信处理部 303

的处理中，发生了某个错误的情况下，这些处理部 301、303 都作成 HTTP 错误消息，并发送到客户端装置 10（步骤 S701）；然后切断与客户端装置 10 的 TCP 连接（步骤 S702）。这里，也可以省略步骤 S701。在步骤 S701 的处理中，各处理部 301、303 也可以作成错误日志文件并把错误理由输出到该文件内。

[0136] 图 11 是图 8 中的高速缓存应答处理（步骤 S408）的详细流程图。

[0137] 网关服务器装置 30 的加密通信处理部 303（参照图 3），在 SSL 加密通信中继处理的步骤 S504（参照图 9）等中，进行加密通信时的内容的高速缓存，再把高速缓存数据存储在存储器 1002 或辅助存储装置 1005 等内。在高速缓存应答处理（步骤 S408）中，加密通信处理部 303 用该高速缓存数据作成 HTTP 应答数据，用在与客户端装置 10 的 SSL 信号交换时所作成的公共密钥进行加密。然后，把该数据发送到客户端装置 10（步骤 S801）。

[0138] （用户同意确认处理）

[0139] 图 12 是图 4 中的用户同意确认处理（步骤 S600）的详细流程图。所谓用户同意确认处理，是就其用网关服务器装置 30 终止并中继加密通信，用来获得用户的同意的处理。

[0140] 首先，网关服务器装置 30 的加密通信处理部 303（参照图 3），对客户端装置 10，发送重定向到以加密通信处理部 303 为 SSL 服务器的 URL 的指示。作为具体例，应答如下的 HTTP 应答状态（步骤 S601）。

[0141] “HTTP/1.1302Found

[0142] Location ://GatewayServer :443/…

[0143] …”

[0144] 这里，由 Location 字段所表示的值，代表重定向指示目标的 URL。重定向指示目标的 URL 的主机名，取为表示具有加密通信处理部 303 的网关服务 器装置 30 的主机名 ；URL 的模式取为代表 SSL 等的加密通信“https”；也可以没有 URL 的路径部分。另外，加密通信处理部 303，在此动态地作成用户同意确认页，同时也预先作成对应于该页的路径字符串，也可以具有把路径与用户同意确认页对应起来的管理表。

[0145] 然后，HTTP 代理处理部 301，从客户端装置 10 接收对在步骤 S601 指示的重定向目标 URL 的目的地服务器、即针对网关服务器装置 30 自身的 CONNECT（步骤 S602）。

[0146] 接下来，HTTP 代理处理部 301，进行图 4 所示的 CONNECT 接收处理（步骤 S603），这里，在加密通信设定数据库 401 内，网关服务器装置 30 地址的 CONNECT 方法预先作了进行 End-End SSL 加密通信处理那样的设定。具体地说，就是预先作成有这样的表目 4019 ：即在服务器名字段 4011 内是代表具有加密通信处理部 303 的网关服务器装置 30 的主机名所谓“GatewayServer”；在通信方法字段 4012 内是“End-End SSL”通信方法 ；在客户端 IP 地址字段 4013 和有效期限 4014 内是“无指定”；在加密通信中继许可证字段 4015 和秘密密钥字段 4016 内是“无数据”。

[0147] 这样，HTTP 代理处理部 301 就把这里接收到的 CONNECT 方法判定为是送往网关服务器装置 30 自身的“End-End SSL”通信方法的连接请求。然后，HTTP 代理处理部 301，进行用来与加密通信处理部 303 之间进行数据的交换的处理。以下，加密通信处理部 303 进行与客户端装置 10 的通信。HTTP 代理处理部 301，把从加密通信处理部 303 交换的数据，原样发送到客户端装置 10，或者追加或消除客户端装置 10 与 HTTP 代理处理部 301 的通信用的 HTTP 头之后，发送到客户端装置 10。此后，同样把从客户端装置 10 接收到的数据交接

给加密通信处理部 303。

[0148] 然后，加密通信处理部 303，把对 CONNECT 方法的应答发送到客户端装置 10 之后，SSL 信号交换处理（步骤 S604、S605）；而后，在被加过密的状态下，接收针对在步骤 S601 指示的重定向目的地 URL 的访问请求（步骤 S606），并将其解密。

[0149] 接着，加密通信处理部 303，用 SSL 加密用户同意确认页，并发送到客户端装置 10（步骤 S607、S608）。所谓用户同意确认页，是在客户端装置 10 的浏览器上，就其由网关服务器装置 30 终止并中继加密通信，用来进行用户的同意确认的内容。在得到了用户同意的情况下，在加过密的状态下对网关服务器装置 30 发送包含表示用户同意的参数的访问请求（步骤 S609）。

[0150] 在未得到用户同意的情况下，在加过密的状态下发送包含表示访问请求未被送来或用户拒绝的参数的访问请求。在加密通信处理部 303 接收到带拒绝参数的访问请求的情况下，也可以进行不能进行加密通信中继的旨意的应答。另外，把此时的 CONNECT 目标内容服务器装置名存储起来，此后，在从客户端装置 10 接收到 CONNECT 方法的情况下，如果 CONNECT 目标内容服务器装置 20 被以前的同用户拒绝了的场合，也可以在一定时间进行表示拒绝访问的应答。

[0151] 在步骤 S609 接收到访问请求时，在步骤 S607 应答用户同意确认页之后，在经过了规定的限制时间的情况下（步骤 S610 中“否”），进行错误处理（步骤 S109）；否则（步骤 S610 中“是”），加密通信处理部 303，把网关服务器装置 30 的根 CA 证书（自己署名证书）加密并后发送到客户端装置 10（步骤 S611、S612）。

[0152] 这里，为了把下载下来的根 CA 证书安装到客户端装置 10 的浏览器内，也可以使指示用户的语句包含在同意确认页中或发送根 CA 证书之前准备好的其他页内，由此，也可以指示把用户下载下来的根 CA 证书安装到客户端装置 10 的浏览器内。然后结束用户同意确认处理。

[0153] 图 13 是用户同意确认处理中所使用的用户同意确认页的示例图。

[0154] 同意确认页，是客户端装置 10 接收到同意确认页时，客户端装置 10 的浏览器为了把同意确认的语句 102 显示在显示器 101 上所记述的内容。作为具体例子，可以列举出 HTML 页，但是也可以不是文本文档而是显示语句 102 的应用。语句 102，例如，是让用户选择是否许可在网关服务器装置 30 终止和解密加密通信（Split SSL 通信）的消息。

[0155] （补充：附加价值处理例）

[0156] 图 14 是本实施方式中进行附加价值处理的示例图。

[0157] 在本实施方式中，HTTP 代理处理部 301，解析在步骤 S406（参照图 8）的处理解密后的明文的通信数据 601，并检索是否包含特定数据排列 602。图 14 的例子中，检索叫做“Layer7#Tunneling#Protocol/1.0”的字符串。这里，特定数据排列 602 也可以有多种。HTTP 代理处理部 301，在检测到已经完成解密的通信数据 601 中包含有特定数据排列 602 的情况下，就切断该连接。或者在发送了加密过的错误应答之后，切断该连接。

[0158] 即，客户端装置 10 解析访问内容服务器装置 20 时的访问请求的内容，可以检测非法目的的通信或将其切断。同样，对于从客户端装置 10 向内容服务器装置 20 发送的通信数据 601，也可以解析其内容，所以，例如也能够防止在内部网络内作为秘密文档管理的文档被非法或错误地发送到内部网络以外。

[0159] 另外，HTTP 代理处理部 301，解析了在步骤 S503（参照图 9）的处理解密过的通信数据 601 之后，在该通信数据是图象文件的情况下，作为步骤 S504 的处理，进行图象变换。例如，Web 浏览器在不支持某种格式的图象文件的情况下，HTTP 代理处理部 301 将其变换为 Web 浏览器支持的其他格式的图象文件。或者，根据客户端装置 10 的显示器的图象分辨率进行变更图象文件的大小等处理。

[0160] 同样，通过解析从内容服务器装置 20 发送并解过密的通信数据 601，就可以检测出病毒或其他有害的信息。也可以把这种检测有害信息的处理作为附加价值处理。在这种场合，能够防止对连接客户端装置 10 的内部网络的有害信息的侵入。

[0161] （第一实施方式的作用和效果）

[0162] 在本实施方式中，在客户端装置 10 与网关服务器装置 30 之间，和在网关服务器装置 30 与内容服务器装置 20 之间，分别进行加密通信。因此，能够确保客户端装置 10 与内容服务器装置 20 之间的通信的安全性。

[0163] 在本实施方式中，客户端装置 10 与内容服务器装置 20 之间进行的 End-End 加密通信，在网关服务器装置 30 中，暂时终止加密通信，并把加过密的通信消息还原成明文。因此，能够在通信消息中进行病毒或秘密文档的检测处理，并且能够进行内容数据的高速缓存或 HTTP 头和数据的追加、变换、消除等处理。

[0164] 一旦服务器公开密钥证书的验证失败，就由客户端装置 10 的浏览器显示 内容服务器装置 20 不可靠的警告消息，但是有用户不理解警告的含义，无视警告而进行访问的情况。本实施方式中，在步骤 S414 网关服务器装置 30 由代理进行服务器公开密钥证书的验证，并在验证失败时进行错误处理（步骤 S109），从而能够对不可靠的内容服务器装置 20 的访问防患于未然。

[0165] 在通过客户端装置 10 的浏览器，客户端装置 10 下载了不被根 CA 信赖的 CA 发行的服务器公开密钥证书的情况下，客户端装置 10 的浏览器往往在证书验证时发出警告消息来通知用户。另外，还有拒绝向该服务器公开密钥证书表示的内容服务器装置 20 的用加密通信的访问的浏览器。在本实施方式中，因为要进行用户同意确认处理（步骤 S600），用户就要把网关服务器装置 30 的根 CA 证书安装在客户端装置 10 的浏览器内，所以，以后，就能够抑制在下载了网关服务器装置 30 生成的加密通信中继许可证 4015 时所表示的警告消息的显示。而且，在证书验证失败时拒绝加密通信的浏览器中，就能够进行与网关服务器装置 30 的加密通信。

[0166] 在本实施方式中，在网关服务器装置 30 或数据库服务器装置 40 受到存有恶意的第三者攻击侵入的情况下，有可能被有恶意的第三者盗取加密通信中使用的秘密密钥或公共密钥等。因此，通过进行用户同意确认处理，就能够明示地通知用户 :残留有加密通信数据盗听和篡改等危险性。在用户不能容许这种危险性的情况下，或者用户不希望由网关服务器装置 30 终止和解密加密通信的情况下，作为用户同意确认处理中的警告消息的回答，用户可以作出不执行 Split SSL 处理的用户自身的选择。

[0167] 或者，在加密通信设定数据库 401 中，用户使服务器名字段 4011 的通信方法字段 4012 的设定成为可变更，由此，用户就可以对每个目的地服务器选择使用 End-End 加密通信和 Split SSL 加密通信的哪一种。作为其优点，用户自身可以根据用户的意思或通信内容来选择安全性和方便性的其中一方。例如，在用户把信用卡号发送到服务器的场合等要

重视安全性的情况下，可以设定 End-End 加密通信。相反，在网关服务器装置 30 中根据 Web 浏览器的特性要对某个图象内容进行图象变换等、用户要重视方便性的情况下，用户自身可以设定 Split SSL 加密通信。

[0168] 另外，在本实施方式中，在将数据库服务器装置 40 独立于网关服务器装 置 30、并列有多台网关服务器装置 30 的情况下，能够实现网关服务器装置 30 的负荷的分散。而且，由于可以根据来自客户端装置 10 的业务量增设网关服务器装置 30，所以能够将适用本发明的网络系统可缩放地扩大到数据库服务器装置 40 达到性能极限。

[0169] < 第二实施方式 >

[0170] 然后参照 15 详细说明本发明的第二实施方式。

[0171] 图 15 是本发明的第二实施方式中把客户端编成组进行代理认证的情况下的 Split SSL 加密通信处理的流程示例图。在本实施方式中，网关服务器装置 30，对客户端装置 10，进行客户端认证之后，对内容服务器装置 20，使用与客户端装置 10 的客户端证书不同的其他客户端证书（客户端代理证书），来进行对应于客户端装置 10 的客户端认证。

[0172] 图 15 中，网关服务器装置 30 的加密通信处理部 303（参照图 3），对客户端装置 10 发送针对 CONNECT 方法的应答之后，进行 SSL 信号交换处理（步骤 S403 ～ S405）；在该 SSL 信号交换处理中，加密通信处理部 303，进行步骤 S404 之后，从客户端装置 10 接收客户端证书（步骤 S416）；进行客户端认证处理（步骤 S417）；然后，网关服务器装置 30，进行客户端的分类处理（步骤 S418）。

[0173] 作为客户端的分类处理的例子，某客户端 A 可以访问某内容服务器 A，而假设不能访问内容服务器 B，另外，另外的客户端 B 可以访问内容服务器 A 和 B 两方。这里，在接收到来自客户端 A 的客户端证书的情况下，分类为客户端类别 A；在接收到来自客户端 B 的客户端证书的情况下，分类为客户端类别 B。

[0174] 加密通信处理部 303，一旦在步骤 S405 结束与客户端装置 10 的 SSL 信号交换，此后，就在与内容服务器装置 20 之间进行 TCP 连接（步骤 S411）；然后，与内容服务器装置 20 之间进行 SSL 信号交换处理（步骤 S412，即，步骤 S4121 ～ S4125）；这里，加密通信处理部 303，在结束了与内容服务器装置 20 的服务器认证处理（步骤 S4122）之后，选择对应步骤 S418 的客户端分类的客户端代理证书（步骤 S4123）。例如，在先前的例子中，如果客户端装置 10 是客户端 A，就选择客户端类别 A 用的客户端代理证书。

[0175] 然后，加密通信处理部 303，在对内容服务器装置 20 进行客户端认证处理时，取代客户端装置 10 的客户端证书，把在步骤 S4123 选择出来的客户端代理证书发送到内容服务器装置 20（步骤 S4124）；此后，进行通常的 SSL 信号交换处理（步骤 S4124、S4125）；再接下来进行 SSL 加密通信中继处理（步骤 S415）。

[0176] 在本实施方式中，内容服务器装置 20 也就是内容提供商方，无须进行全部的客户端的客户端认证，只对网关服务器装置 30 管理的客户端网络运用者方提供的客户端类别部分的客户端认证就可以。例如，在是 1000 万人加入的 ISP 网络系统的情况下，原来，内容提供者方为了要区别 1000 万人来认证客户端，内容服务器装置 20（内容提供商），必须要用来认证 1000 万人的大规模的认证管理系统。而在本实施方式中，由网关服务器装置 30 汇总用代理进行客户端认证，所以，内容提供商仅引入小规模的认证系统即可。

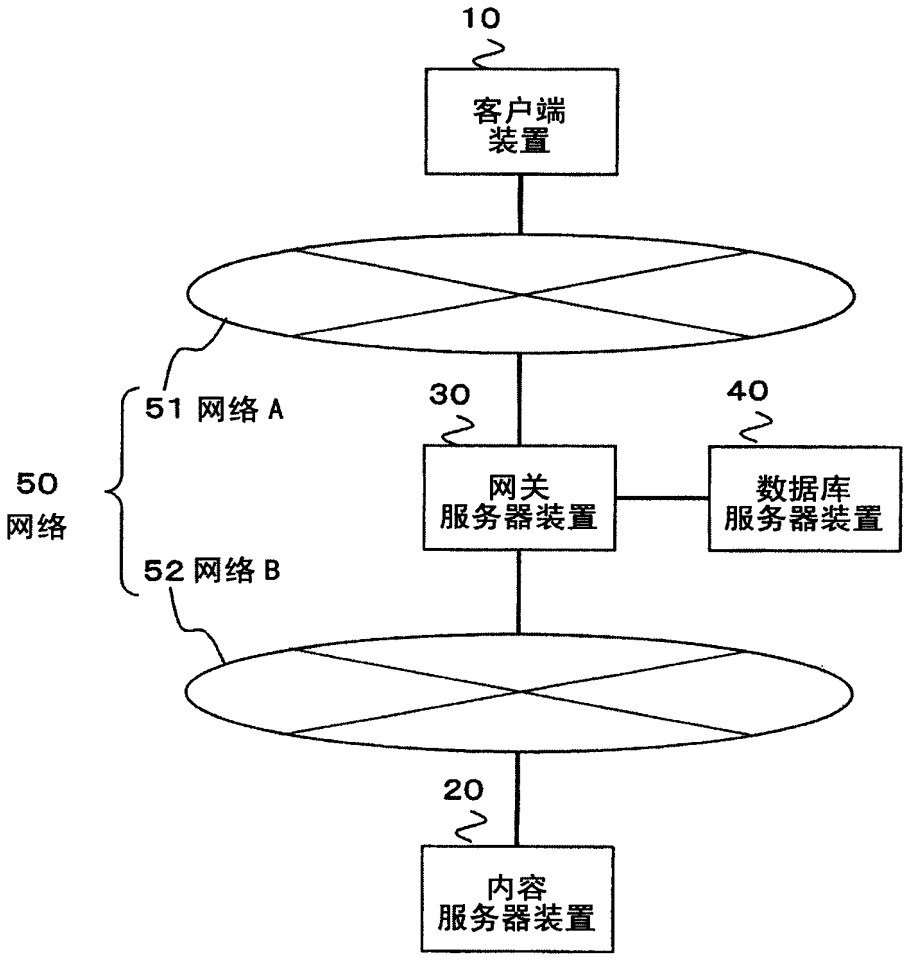


图 1

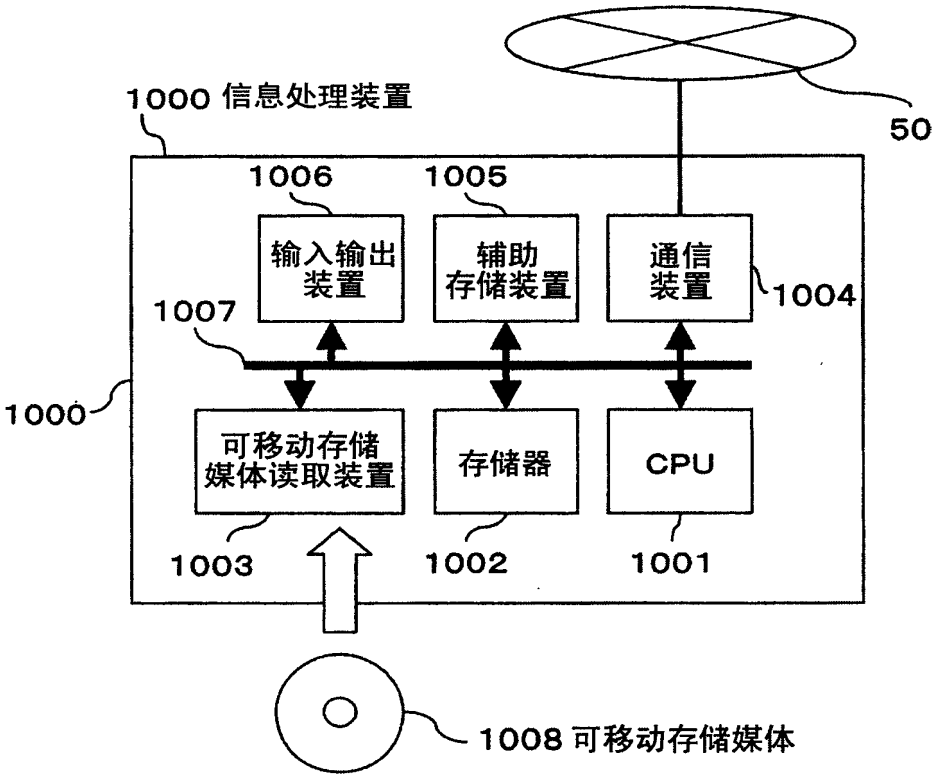

1000 信息处理装置
50
1006
1005
输入输出装置
辅助存储装置
通信装置
1004
1007
1000
可移动存储媒体读取装置
存储器
CPU
1003
1002
1001
1008 可移动存储媒体

图 2

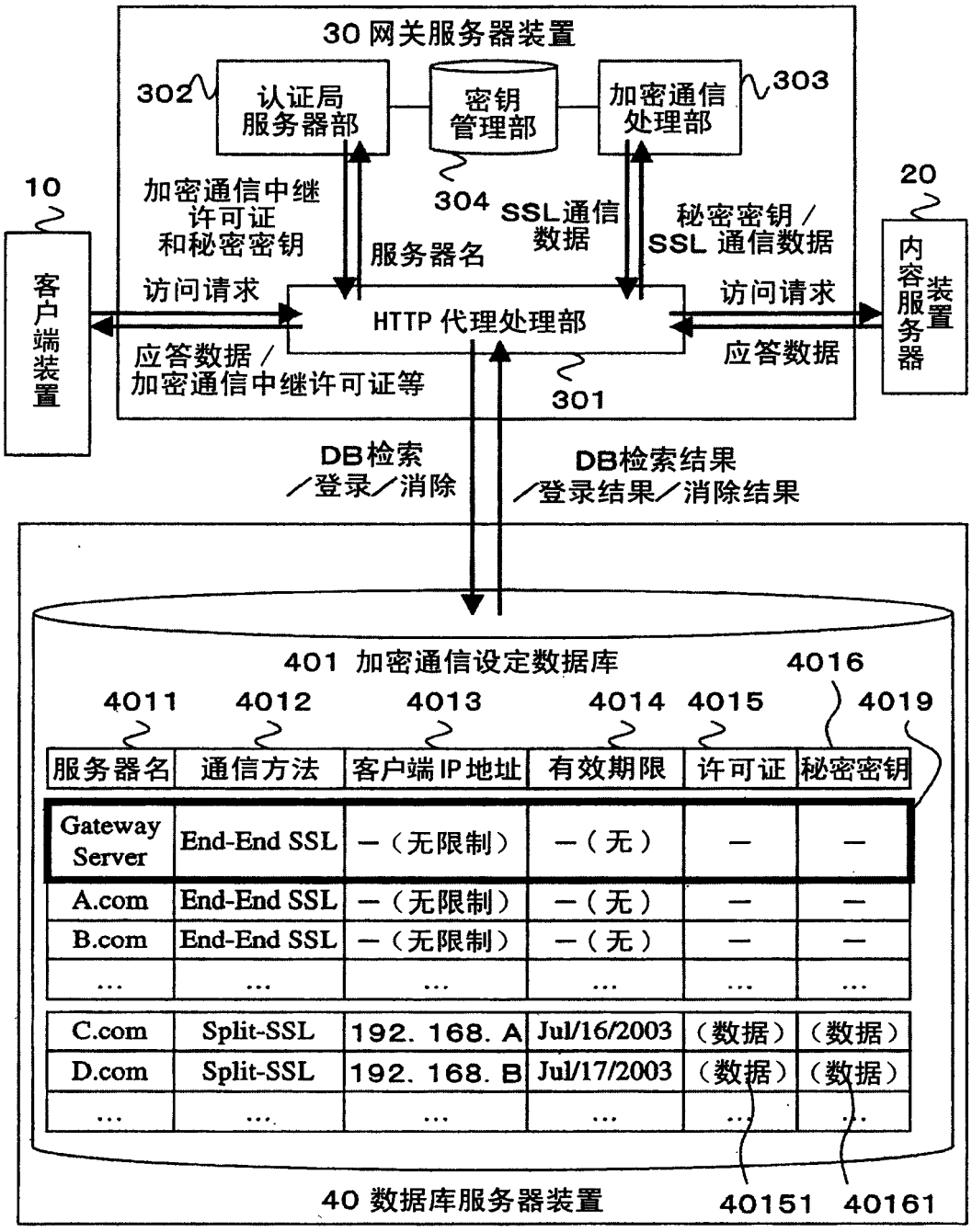

30 网关服务器装置
302
认证局
服务器部
密钥
管理部
304
加密通信
处理部
303
10
客户端装置
加密通信中继
许可证
和秘密密钥
服务器名
SSL通信
数据
秘密密钥 /
SSL 通信数据
20
内容服务器装置
访问请求
HTTP 代理处理部
访问请求
应答数据 /
加密通信中继许可证等
应答数据
301
DB检索
/登录/消除
DB检索结果
/登录结果/消除结果
401 加密通信设定数据库
4016
4011
4012
4013
4014
4015
4019
服务器名
通信方法
客户端IP地址
有效期限
许可证
秘密密钥
Gateway Server
End-End SSL
—（无限制）
—（无）
—
—
A.com
End-End SSL
—（无限制）
—（无）
—
—
B.com
End-End SSL
—（无限制）
—（无）
—
—
…
…
…
…
…
…
C.com
Split-SSL
192. 168. A
Jul/16/2003
（数据）
（数据）
D.com
Split-SSL
192. 168. B
Jul/17/2003
（数据）
（数据）
…
…
…
…
…
…
40 数据库服务器装置
40151
40161

图 3

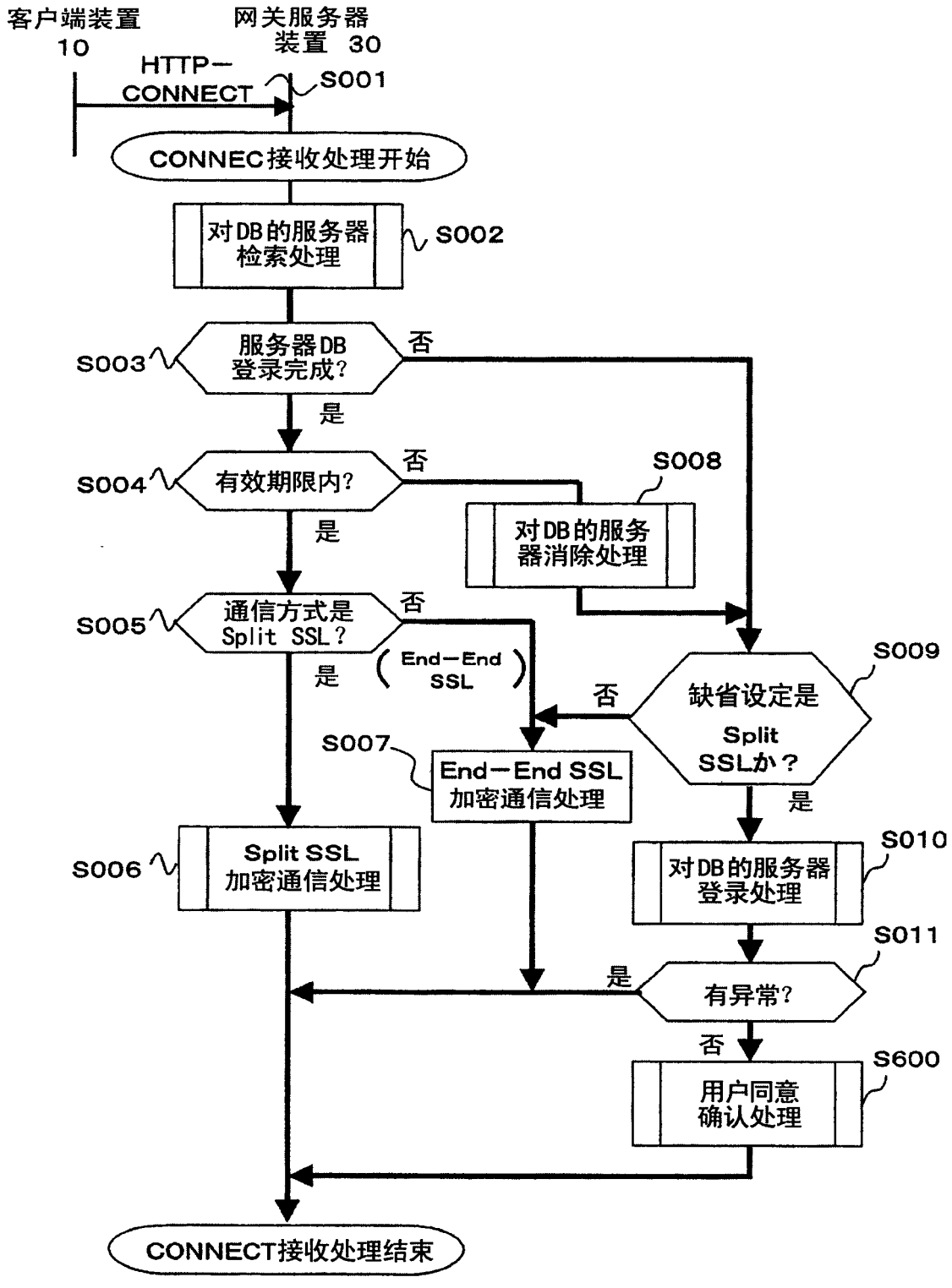

客户端装置
10
网关服务器
装置 30
HTTP—
CONNECT
S001
CONNEC接收处理开始
对DB的服务器
检索处理
S002
服务器DB
登录完成?
S003
否
是
有效期限内?
S004
否
是
S008
对DB的服务
器消除处理
通信方式是
Split SSL?
S005
否
是
End—End
SSL
缺省设定是
Split
SSL か?
S009
否
是
S007
End—End SSL
加密通信处理
Split SSL
加密通信处理
S006
对DB的服务器
登录处理
S010
有异常?
S011
是
否
用户同意
确认处理
S600
CONNECT接收处理结束

图 4

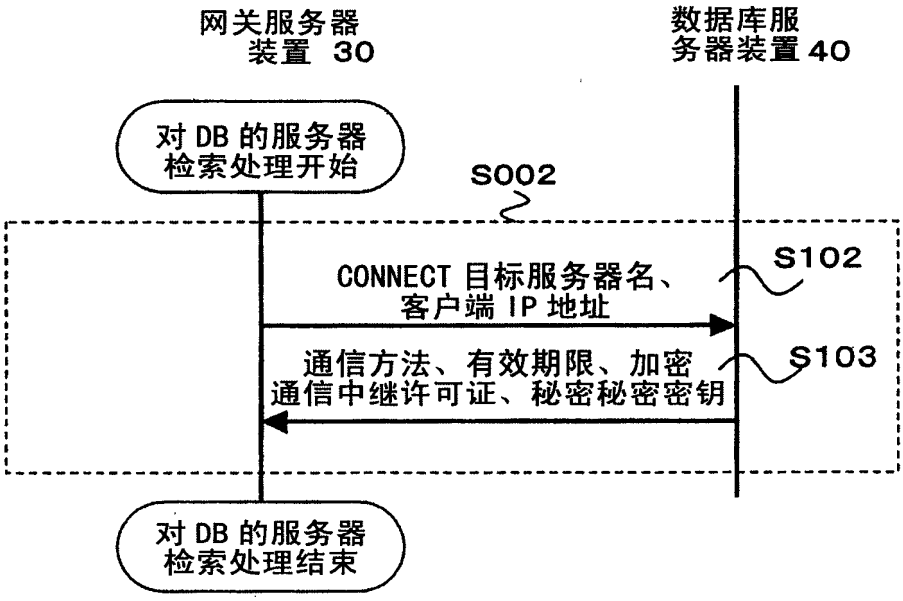

网关服务器
装置 30
数据库服
务器装置 40
对 DB 的服务器
检索处理开始
S002
CONNECT 目标服务器名、
客户端 IP 地址
S102
通信方法、有效期限、加密
通信中继许可证、秘密秘密密钥
S103
对 DB 的服务器
检索处理结束

图 5

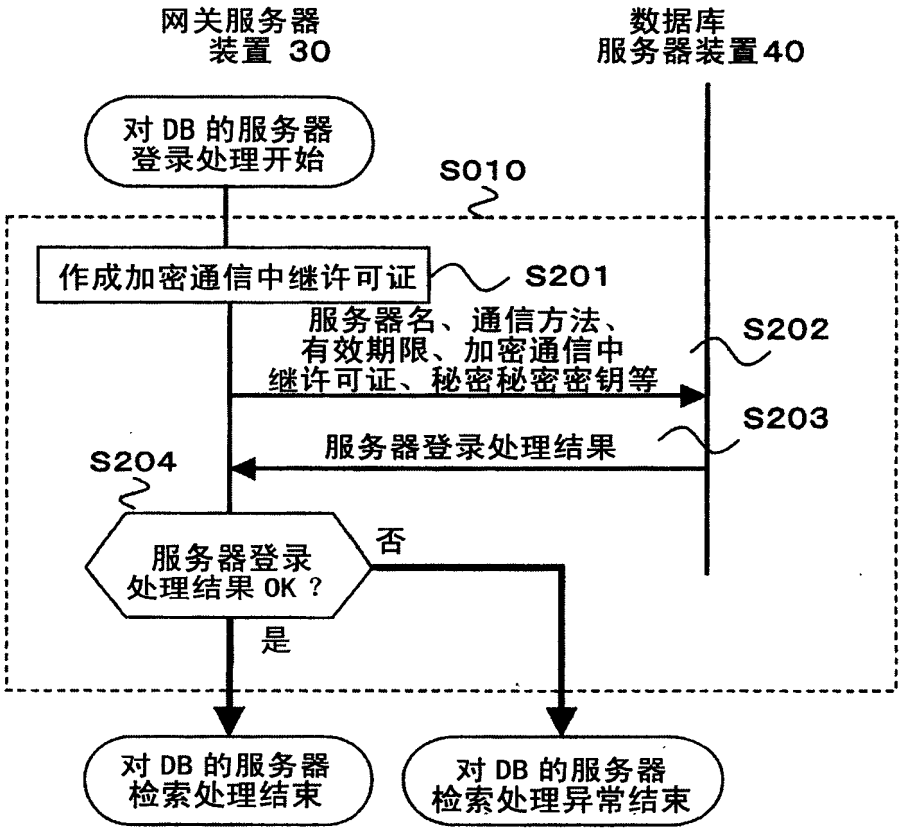

网关服务器
装置 30
数据库
服务器装置 40
对 DB 的服务器
登录处理开始
S010
作成加密通信中继许可证
S201
服务器名、通信方法、
有效期限、加密通信中
继许可证、秘密秘密密钥等
S202
服务器登录处理结果
S203
S204
服务器登录
处理结果 OK ？
否
是
对 DB 的服务器
检索处理结束
对 DB 的服务器
检索处理异常结束

图 6

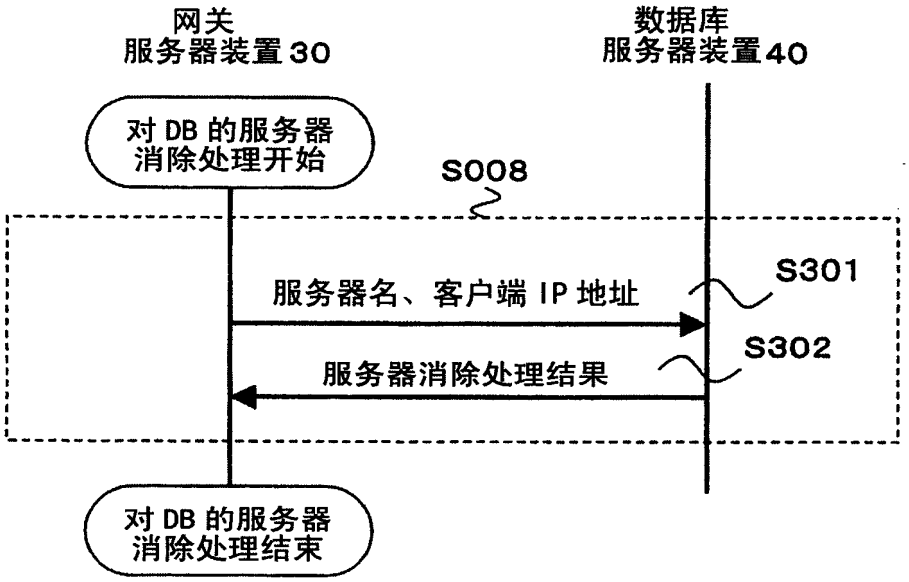

网关
服务器装置30
数据库
服务器装置40
对DB的服务器
消除处理开始
S008
服务器名、客户端IP地址
S301
S302
服务器消除处理结果
对DB的服务器
消除处理结束

图 7

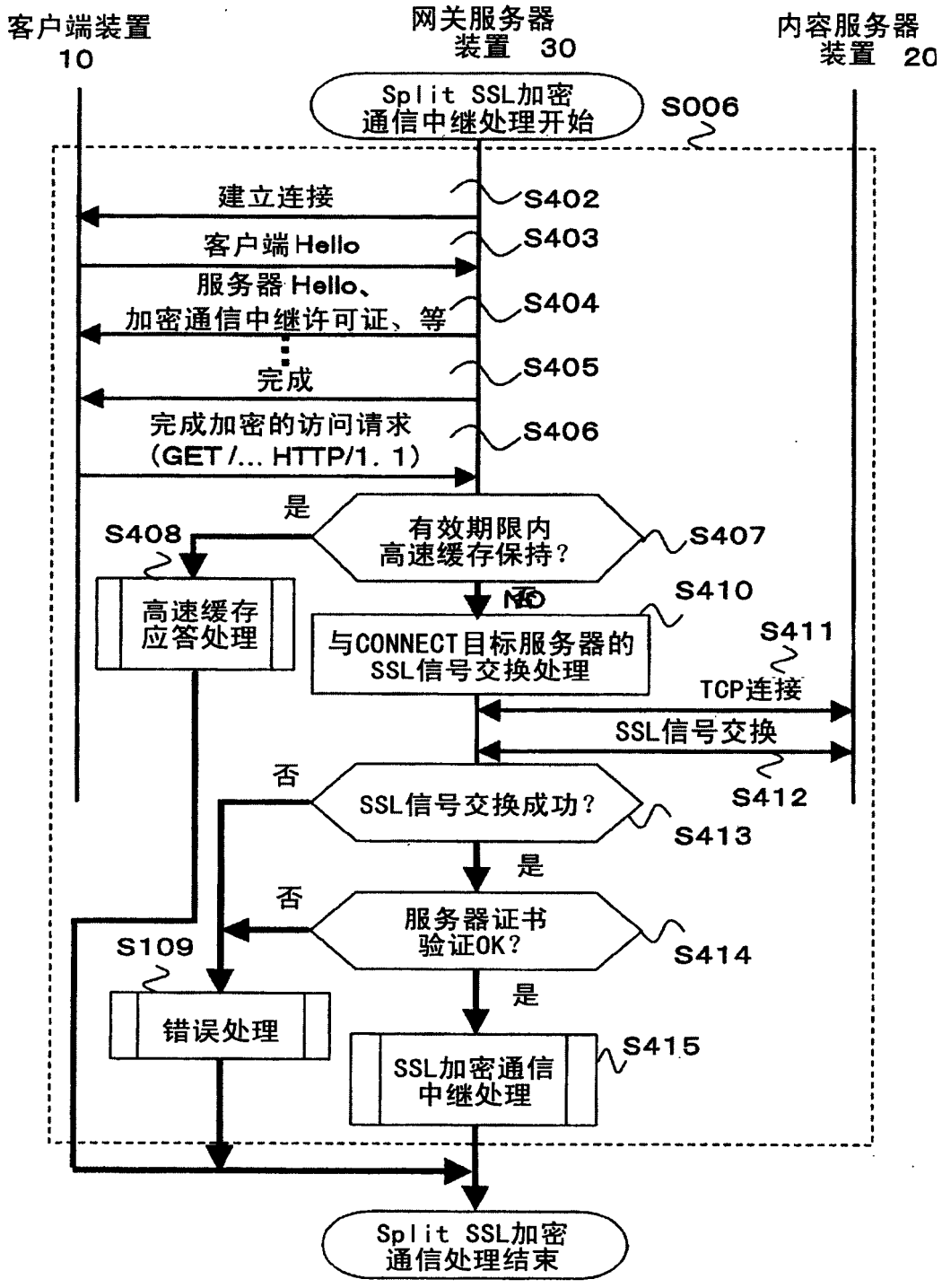

客户端装置
10
网关服务器
装置 30
内容服务器
装置 20
Split SSL加密
通信中继处理开始
S006
建立连接
S402
客户端Hello
S403
服务器Hello、
加密通信中继许可证、等
S404
完成
S405
完成加密的访问请求
(GET /... HTTP/1. 1)
S406
是
有效期限内
高速缓存保持?
S407
S408
高速缓存
应答处理
否
S410
与CONNECT目标服务器的
SSL信号交换处理
S411
TCP连接
SSL信号交换
S412
否
SSL信号交换成功?
S413
是
否
服务器证书
验证OK?
S414
S109
错误处理
是
SSL加密通信
中继处理
S415
Split SSL加密
通信处理结束

图 8

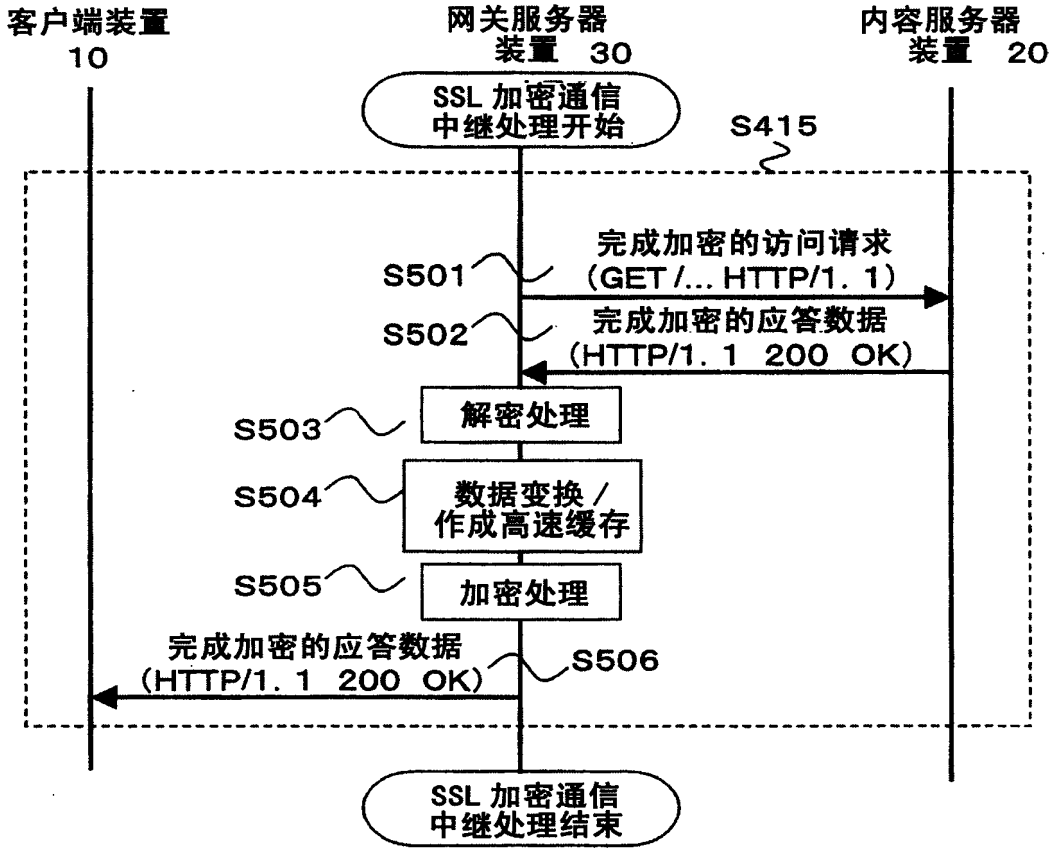

客户端装置
10
网关服务器
装置 30
内容服务器
装置 20
SSL 加密通信
中继处理开始
S415
S501
完成加密的访问请求
(GET /... HTTP/1. 1)
S502
完成加密的应答数据
(HTTP/1. 1 200 OK)
S503
解密处理
S504
数据变换 /
作成高速缓存
S505
加密处理
完成加密的应答数据
(HTTP/1. 1 200 OK)
S506
SSL 加密通信
中继处理结束

图 9

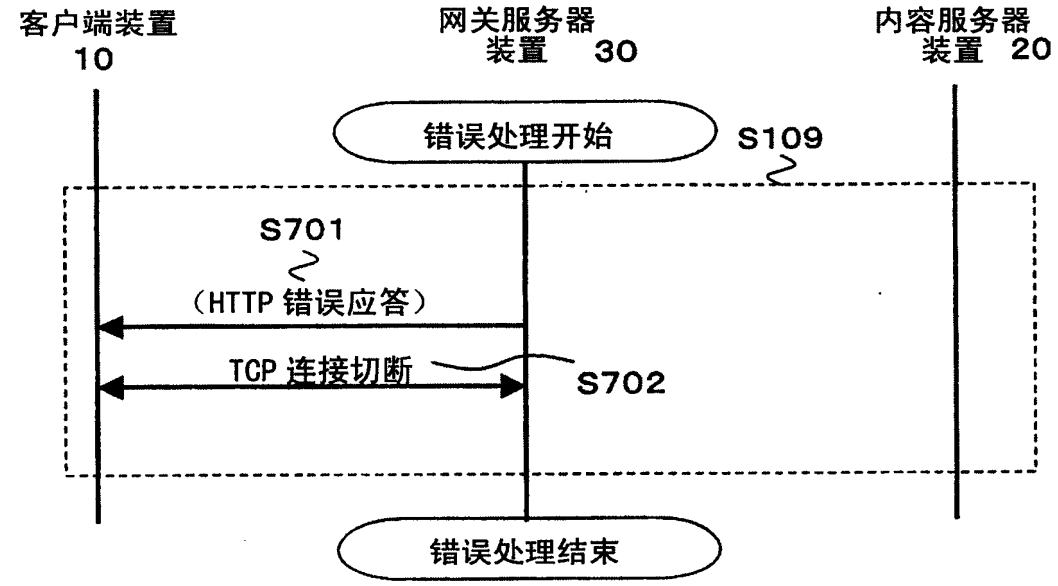

客户端装置
10
网关服务器
装置 30
内容服务器
装置 20
错误处理开始
S109
S701
(HTTP 错误应答)
TCP 连接切断
S702
错误处理结束

图 10

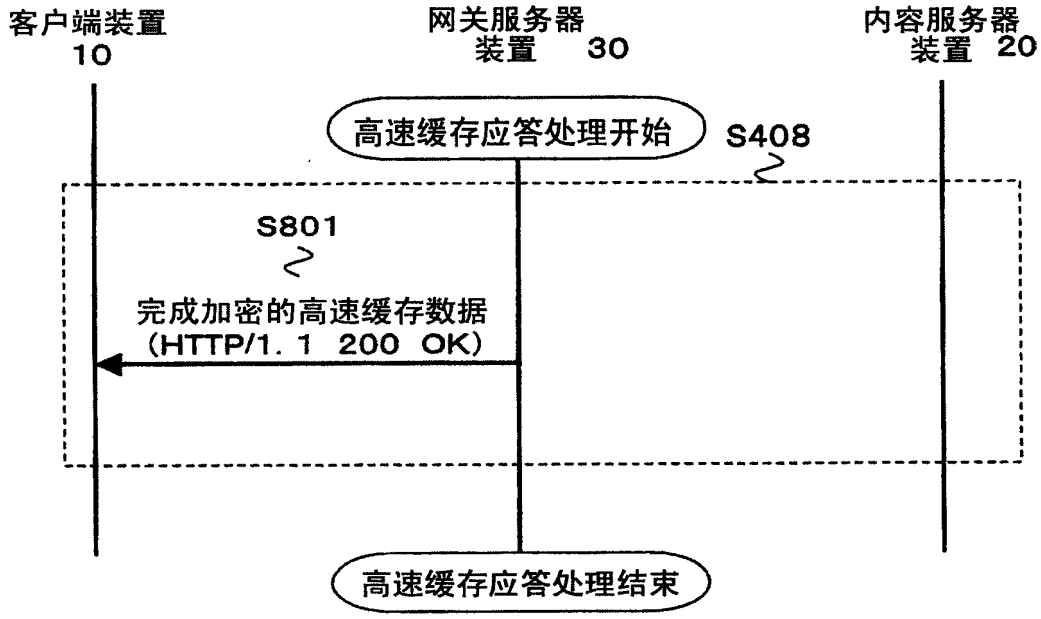

客户端装置
10
网关服务器
装置 30
内容服务器
装置 20
高速缓存应答处理开始
S408
S801
完成加密的高速缓存数据
(HTTP/1.1 200 OK)
高速缓存应答处理结束

图 11

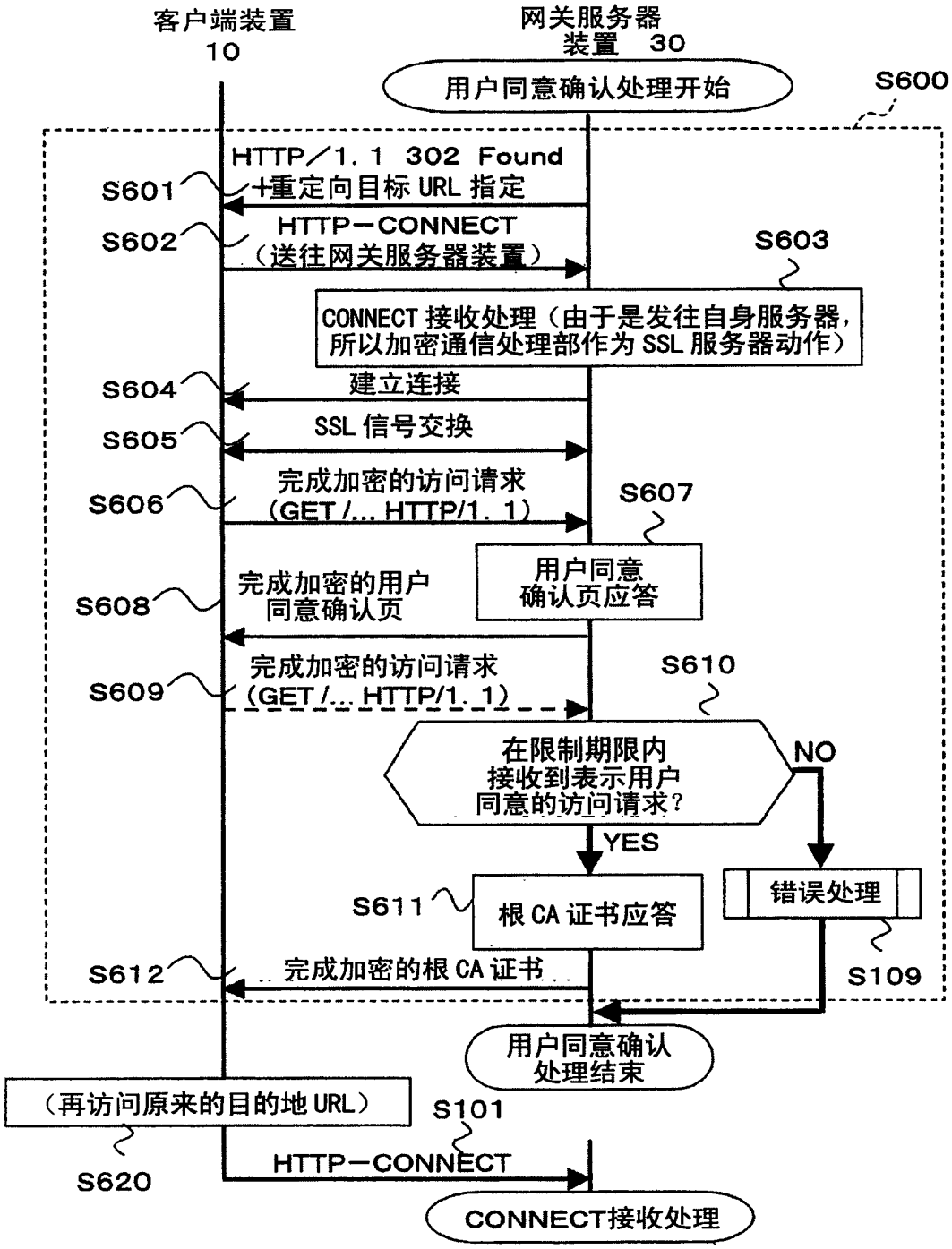

客户端装置
10
网关服务器
装置 30
用户同意确认处理开始
S600
HTTP／1.1 302 Found
+重定向目标 URL 指定
S601
HTTP－CONNECT
（送往网关服务器装置）
S602
S603
CONNECT 接收处理（由于是发往自身服务器，
所以加密通信处理部作为 SSL 服务器动作）
S604
建立连接
S605
SSL 信号交换
完成加密的访问请求
（GET /... HTTP/1.1）
S606
S607
用户同意
确认页应答
完成加密的用户
同意确认页
S608
完成加密的访问请求
（GET /... HTTP/1.1）
S609
S610
在限制期限内
接收到表示用户
同意的访问请求？
NO
YES
S611
根 CA 证书应答
错误处理
S612
完成加密的根 CA 证书
S109
用户同意确认
处理结束
（再访问原来的目的地 URL）
S101
S620
HTTP－CONNECT
CONNECT接收处理

图 12

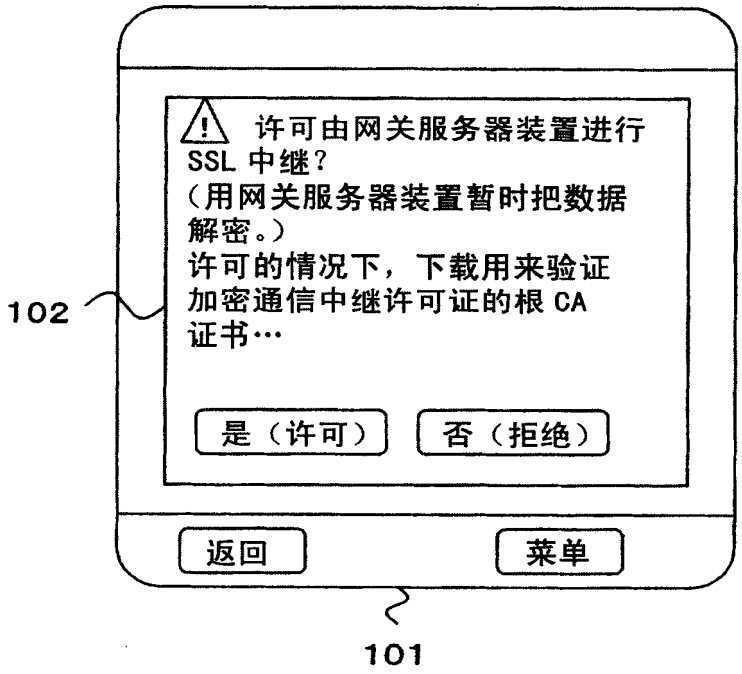

许可由网关服务器装置进行SSL 中继？
（用网关服务器装置暂时把数据解密。）
许可的情况下，下载用来验证加密通信中继许可证的根 CA 证书…
是（许可）
否（拒绝）
返回
菜单
102
101

图 13

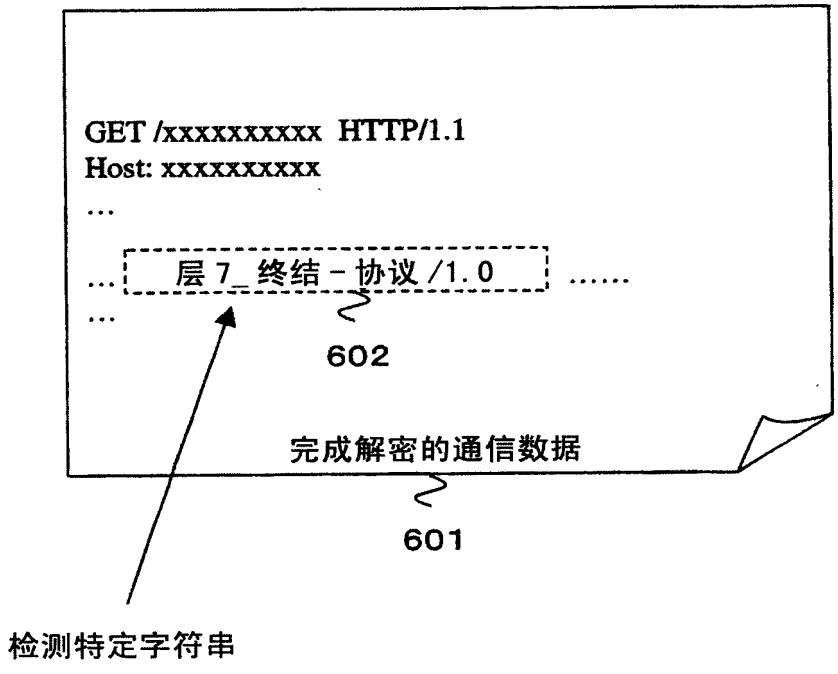

GET /xxxxxxxxxx HTTP/1.1
Host: xxxxxxxxxx
…
… 层 7_ 终结 - 协议 /1.0 ……
…
602
完成解密的通信数据
601
检测特定字符串

图 14

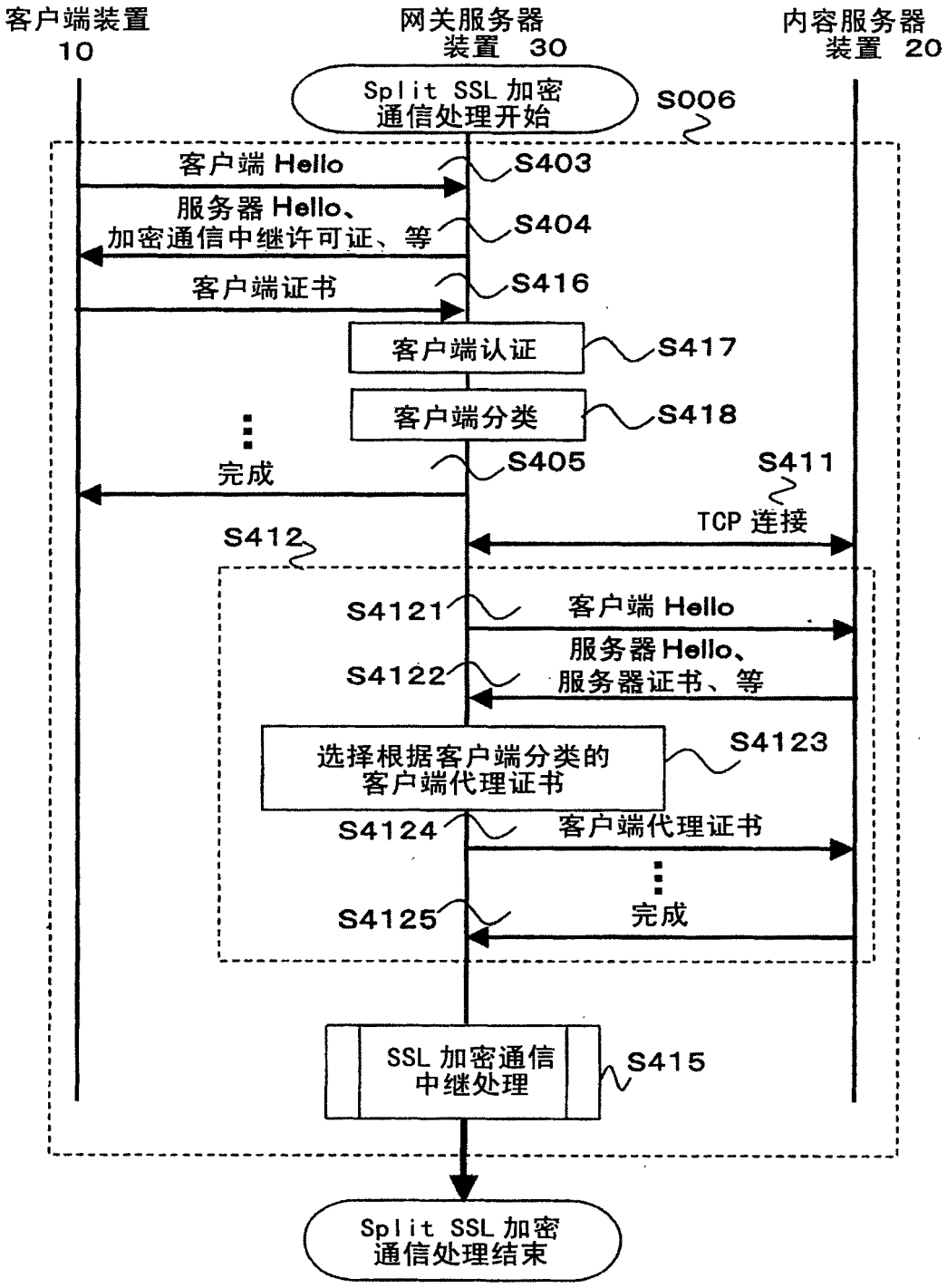

客户端装置
10
网关服务器
装置 30
内容服务器
装置 20
Split SSL 加密
通信处理开始
S006
客户端 Hello
S403
服务器 Hello、
加密通信中继许可证、等
S404
客户端证书
S416
客户端认证
S417
客户端分类
S418
完成
S405
S411
TCP 连接
S412
S4121
客户端 Hello
服务器 Hello、
服务器证书、等
S4122
选择根据客户端分类的
客户端代理证书
S4123
S4124
客户端代理证书
完成
S4125
SSL 加密通信
中继处理
S415
Split SSL 加密
通信处理结束

图 15