[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 17/00
G06F 11/30 G06F 12/14
G06F 13/00 G06F 9/06

[12] 发明专利申请公开说明书

[21] 申请号 02128619.1

[43] 公开日 2003 年 2 月 5 日

[11] 公开号 CN 1395191A

[22] 申请日 2002.5.28 [21] 申请号 02128619.1

[30] 优先权

[32] 2001.6.28 [33] JP [31] 195688/2001

[32] 2002.5.27 [33] JP [31] 151711/2002

[71] 申请人 株式会社日立制作所

地址 日本东京都

[72] 发明人 青岛弘和 吉浦裕 宇贺神敦
镰田英一 渡边直树

[74] 专利代理机构 中国专利代理(香港)有限公司

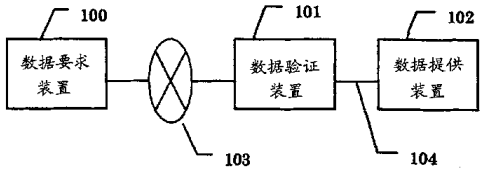
代理人 吴立明 王忠忠

权利要求书 4 页 说明书 18 页 附图 9 页

[54] 发明名称 数据验证方法、数据验证装置及其处理程序产品

[57] 摘要

本发明提供一种能够防止从数据提供装置所发送的数据被篡改和本不应公开的数据被提供给数据要求装置的技术，在连接数据要求装置和数据提供装置的网络上设置数据验证装置，在数据验证装置中验证与所要求的提供数据相对应的验证数据与提供数据是否相一致，根据验证结果，变更从数据验证装置向数据要求装置发送的数据。



ISSN1008-4274

1. 一种数据验证装置中的数据验证方法，根据要求验证从数据验证装置所发送的数据，其特征在于，包括：

从数据要求装置接收包含数据的识别符的数据要求的要求接收步骤；

根据上述识别符来取得用于验证的验证数据的验证数据取得步骤；

根据接收的要求向数据提供装置发送上述所要求的数据的提供要求的要求发送步骤；

根据上述提供要求接收数据提供装置发送的提供数据的数据接收步骤；

根据上述验证数据来验证在数据接收步骤中接收的提供数据的数据验证步骤；

根据上述数据验证步骤的结果来控制对数据要求装置的数据发送的数据发送控制步骤。

2. 根据权利要求 1 所述的数据验证方法，其特征在于，根据上述识别符，上述验证数据包含能够验证上述提供数据未被改变的数据。

3. 根据权利要求 1 所述的数据验证方法，其特征在于，

上述数据验证步骤是判断上述提供数据是否是上述所要求的数据的步骤，

上述数据发送控制步骤包含下列步骤：

当上述验证结果表示上述提供数据是上述所要求的数据时，发送上述发送数据，当表示上述提供数据与上述所要求的数据不同时，不发送上述提供数据。

4. 根据权利要求 3 所述的数据验证方法，其特征在于，上述数据发送步骤进一步包含下列步骤：

当上述验证结果表示上述提供数据与上述所要求的数据不同时，发送通知不能发送上述所要求的数据的通知数据。

5. 根据权利要求 3 所述的数据验证方法，其特征在于，上述数据发送步骤进一步包含代替数据发送步骤：当上述验证结果表示上述提供数据与上述所要求的数据不同时，把上述所要求的数据置换为代替数据。

6. 根据权利要求 1 所述的数据验证方法，其特征在于，上述验证数据进一步包含用于与对应于上述识别符所发送的提供数据一起来验证将要验证的关联数据的信息。

7. 根据权利要求6所述的数据验证方法，其特征在于，

数据接收步骤进一步包括关联数据取得步骤，从上述数据提供装置接收上述提供数据和将要验证的关联数据，

上述数据验证步骤进一步包括根据上述验证数据来进行上述关联数据的验证的步骤，

上述数据发送控制步骤包含下列步骤：

当上述关联数据验证结果表示上述关联数据是应当作为上述关联数据所取得的数据时，发送上述发送数据，当表示上述关联数据与作为上述关联数据所取得的数据不同时，不发送上述提供数据。

8. 根据权利要求1所述的数据验证方法，其特征在于，与数据的识别符相对应地保存从数据提供装置接收的提供数据。

9. 根据权利要求3所述的数据验证方法，其特征在于，当上述验证结果表示上述提供数据是上述所要求的数据时，给上述提供数据对应地附加数据的识别符来进行保存。

10. 根据权利要求9所述的数据验证方法，其特征在于，当保存的提供数据满足预定的条件时，不执行要求发送步骤。

11. 根据权利要求7所述的数据验证方法，其特征在于，当上述关联数据满足预定条件时，给上述提供数据对应地附加数据的识别符来进行保存。

12. 根据权利要求7所述的数据验证方法，其特征在于，当保存的关联数据满足预定条件时，不执行关联数据取得步骤。

13. 根据权利要求1所述的数据验证方法，其特征在于，在上述数据验证步骤中，验证对提供数据进行预定的处理的结果。

14. 根据权利要求13所述的数据验证方法，其特征在于，对提供数据进行的处理是去除了提供数据的预定部分的处理。

15. 根据权利要求1所述的数据验证方法，其特征在于，进行与数据要求装置的通信的通信协议与进行与数据提供装置的通信的通信协议不同。

16. 根据权利要求1所述的数据验证方法，其特征在于，

当从数据提供装置向数据要求装置所发送的数据被加密时，

在数据验证装置中包括数据提供装置具有的加密所需要的信息，

在数据验证装置中把上述加密而发送的数据根据上述加密所需要的信息进行

解码来复原，

验证上述解码的数据。

17. 根据权利要求 16 所述的数据验证方法，其特征在于，上述加密所需要的信息可以是加密键。

18. 根据权利要求 17 所述的数据验证方法，其特征在于，上述加密键可以是公开键加密系统的专用加密键。

19. 根据权利要求 17 所述的数据验证方法，其特征在于，

在数据要求装置与数据提供装置之间交换加密所需要的信息，

并且，在上述交换中，对于加密所需要的信息中的至少一个，

当数据要求装置用数据提供装置的加密键进行加密而发送时，

数据验证装置用上述加密键对上述加密并发送的信息进行解码并保持，

在以后的通信中，根据上述保持的信息来对加密发送的数据进行解码。

20. 根据权利要求 16 所述的数据验证方法，其特征在于，当上述验证结果表示上述提供数据是上述所要求的数据时，向数据要求装置发送数据提供装置发送的被加密的提供数据。

21. 根据权利要求 16 所述的数据验证方法，其特征在于，当上述验证结果表示上述提供数据与上述所要求的数据不同时，根据上述加密所需要的信息，对通知不能发送上述所要求的数据的通知数据进行加密来发送。

22. 根据权利要求 16 所述的数据验证方法，其特征在于，当上述验证结果表示上述提供数据与上述所要求的数据不同时，根据上述加密所需要的信息，对与上述所要求的数据相对应的代替数据进行加密来发送

23. 一种数据验证装置，根据要求验证从数据提供装置所发送的数据，其特征在于，包括：

要求接收装置，从数据要求装置接收包含数据的识别符的数据要求；

验证数据取得装置，根据上述识别符来取得用于验证的验证数据；

要求发送装置，根据接收的要求，向数据提供装置发送上述所要求的数据的提供要求；

数据接收装置，根据上述提供要求，接收数据提供装置发送的提供数据；

数据验证装置，根据上述验证数据来验证由数据接收装置接收的提供数据；

数据发送控制装置，根据上述数据验证装置的结果，控制对数据要求装置的

数据验证方法、数据验证装置及其处理程序产品

背景技术

本发明涉及验证发送数据的数据验证方法，特别是涉及验证对 WWW（World Wide Web）系统中从 Web 服务器所发送的数据的可靠性，适用于数据验证装置的有效的技术。

近年来，使用 WWW 系统的数据发送被广泛使用。一方面，报告了：在 WWW 系统中对于公开数据的 Web 服务器装置不正当侵入，而使所公开的数据被篡改的事件和在 Web 服务器中错误登录数据，使本不应公开的数据被公开的事件等。当这样的事件发生时，由 Web 服务器所公开的数据的可靠性降低，而存在大大损害通过该 Web 服务器公开数据的企业和团体等的信誉的情况。

对此，存在定期监视由 Web 服务器所公开的数据，来发现篡改的技术。该技术记载在例如日本专利公开公报特开平 11－154139 号「篡改修正方法、篡改修正装置及篡改判定装置」中。其概要是：定期地获得在网络上的预定的位置上所公开的内容，每次判定上述内容是否被篡改。

而且，作为保证数据的可靠性的技术，具有「MONITORING INTEGRITY OF TRANSMITTED DATA」（PCT/IL99/00203）。

当由 Web 服务器所公开的数据受到篡改或者本不应公开的数据被公开时，存在损害在 Web 服务器上公开信息的团体和企业等的信用的情况。即使定期地进行监视，也不能防止在监视与监视之间的时间内发生的篡改和本不应公开的信息的流出。

发明概述

本发明提供能够防止被篡改的数据和本不应公开的数据被提供给数据要求装置的技术。

具体地说，设置数据验证装置来执行以下处理：

设置要求接收步骤，来把握数据要求装置要求哪个数据。

而且，设置验证数据取得步骤，取得成为验证所提供的数据根据的验证数据。

数据发送。

24. 一种数据验证程序，根据要求验证从数据提供装置所发送的数据，其特征在于，上述程序通过读取到计算机上来执行，在上述计算机上构筑实施以下步骤的装置：

要求接收步骤，从数据要求装置接收包含数据的识别符的数据要求；

验证数据取得步骤，根据上述识别符来取得用于验证的验证数据；

要求发送步骤，根据接收的要求，向数据提供装置发送上述所要求的数据的提供要求；

数据接收步骤，根据上述提供要求，接收数据提供装置发送的提供数据；

数据验证步骤，根据上述验证数据来验证由数据接收装置接收的提供数据；

数据发送控制步骤，根据上述数据验证步骤的结果，控制对数据要求装置的数据发送。

而且，设置要求发送步骤和数据接收步骤，取代数据要求装置从数据提供装置取得数据要求装置要求的数据。由此，数据要求装置不会直接取得数据，而能够在向数据要求装置发送数据之前，进行验证处理。

接着，设置数据验证步骤，核对从数据提供装置取得的提供数据和验证数据来进行验证。

接着，当在数据验证步骤中通过使用验证数据的验证而确认了提供数据的正当性的情况下，在数据发送步骤中，向数据要求装置发送数据要求装置要求的数据作为发送数据。

更具体地说，上述正当性的确认是指表示提供数据是所要求的数据的情况。

上述验证数据包含能够根据上述识别符来验证发送的提供数据没有被改变的数据，因此，能够进行提供数据的改变有无的验证。

根据这样的一种形式，本发明提供一种数据验证装置中的数据验证方法，根据要求验证从数据验证装置所发送的数据，其特征在于，包括：从数据要求装置接收包含数据的识别符的数据要求的要求接收步骤；根据上述识别符来取得用于验证的验证数据的验证数据取得步骤；根据接收的要求向数据提供装置发送上述所要求的数据的提供要求的要求发送步骤；根据上述提供要求接收数据提供装置发送的提供数据的数据接收步骤；根据上述验证数据来验证在数据接收步骤中接收的提供数据的数据验证步骤；根据上述数据验证步骤的结果来控制对数据要求装置的数据发送的数据发送控制步骤。

而且，在本发明中，其特征在于，根据上述识别符，上述验证数据包含能够验证上述提供数据未被改变的数据。

而且，在本发明中，其特征在于，上述数据验证步骤是判断上述提供数据是否是上述所要求的数据的步骤，上述数据发送控制步骤包含下列步骤：当上述验证结果表示上述提供数据是上述所要求的数据时，发送上述发送数据，当表示上述提供数据与上述所要求的数据不同时，不发送上述提供数据。

而且，本发明的特征在于，包含下列步骤：当上述验证结果表示上述提供数据与上述所要求的数据不同时，发送通知不能发送上述所要求的数据的通知数据。

而且，在本发明中，其特征在于，上述数据发送步骤进一步包含代替数据发送步骤：当上述验证结果表示上述提供数据与上述所要求的数据不同时，把上述

所要求的数据置换为代替数据。

而且，本发明的特征在于，上述验证数据进一步包含用于与对应于上述识别符所发送的提供数据一起来验证将要验证的关联数据的信息。

而且，在本发明中，其特征在于，数据接收步骤进一步包括关联数据取得步骤，从上述数据提供装置接收上述提供数据和将要验证的关联数据，上述数据验证步骤进一步包括根据上述验证数据来进行上述关联数据的验证的步骤，上述数据发送控制步骤包含下列步骤：当上述关联数据验证结果表示上述关联数据是应当作为上述关联数据所取得的数据时，发送上述发送数据，当表示上述关联数据与作为上述关联数据所取得的数据不同时，不发送上述提供数据。

而且，本发明的特征在于，与数据的识别符相对应地保存从数据提供装置接收的提供数据。

而且，本发明的特征在于，当上述验证结果表示上述提供数据是上述所要求的数据时，给上述提供数据对应地附加数据的识别符来进行保存。

而且，在本发明中，其特征在于，当保存的提供数据满足预定的条件时，不执行要求发送步骤。

而且，在本发明中，其特征在于，当上述关联数据满足预定条件时，给上述提供数据对应地附加数据的识别符来进行保存。

而且，在本发明中，其特征在于，当保存的关联数据满足预定条件时，不执行关联数据取得步骤。

而且，在本发明中，其特征在于，在上述数据验证步骤中，验证对提供数据进行预定的处理的结果。

而且，在本发明中，其特征在于，对提供数据进行的处理是去除了提供数据的预定部分的处理。

而且，在本发明中，其特征在于，进行与数据要求装置的通信的通信协议与进行与数据提供装置的通信的通信协议不同。

而且，当在数据验证步骤中不能确认提供数据的正当性时，在数据发送步骤中不发送提供数据，因此，当提供数据的正当性不能确认时，防止向数据要求装置发送提供数据。

而且，当在数据验证步骤中不能确认提供数据的正当性时，在数据发送步骤中发送表示不能发送提供数据的数据。因此，当提供数据的正当性不能确认时，

防止向数据要求装置发送提供数据，同时，向数据要求装置或者经过网络路径的装置通知不发送提供数据的理由。

而且，当在数据验证步骤中不能确认提供数据的正当性时，在数据发送步骤中把提供数据置换为预定的数据来进行发送。通过使预定的数据例如对不能发送数据的行为成为道歉提示，至少防止了受到改变的数据和本不应公开的信息流出。

而且，通过与提供数据的验证相配合来进行关联数据的验证，在关联数据被改变的情况下，能够取消提供数据的发送。

而且，可以在验证处理之前对提供数据进行预定的处理。

而且，可以从提供数据中去除预定的数据部分，而从验证对象中去除验证对象外的数据部分。

而且，作为连接在网络上的数据验证装置来实现该方法，如果为具有两个以上的网络连接部的装置，数据要求装置和数据提供装置经过该装置来进行通信，因此，数据验证装置进行数据要求装置的要求和从数据提供装置所发送的提供数据的中继。

而且，本发明是，在数据验证装置中包括数据提供装置具有的加密所需要的信息，在数据验证装置中把上述加密而发送的数据根据上述加密所需要的信息进行解码来复原，验证上述解码的数据。

而且，在本发明中，上述加密所需要的信息可以是加密键。

而且，在本发明中，上述加密键可以是公开键加密系统的专用加密键。

而且，在本发明中，数据验证装置用上述加密键来对上述加密而发送的信息进行解码并保持，在以后的通信中，根据上述保持的信息来对加密而发送的数据进行解码。

而且，在本发明中，当上述验证结果表示上述提供数据是上述所要求的数据时，向数据要求装置发送数据提供装置发送的加密后的提供数据。

而且，在本发明中，当上述验证结果表示上述提供数据与上述所要求的数据不同时，根据上述加密所需要的信息，对通知不能发送上述所要求的数据的通知数据进行加密来发送。

而且，在本发明中，当上述验证结果表示上述提供数据与上述所要求的数据不同时，根据上述加密所需要的信息，对上述所要求的数据相对应的代替数据进

行加密来发送。

附图的简要说明

图1是表示包括数据验证装置的网络构成的例子的图;

图2是表示数据验证装置的内部构成的例子的图;

图3是表示包含数据验证装置的处理流程的例子的图;

图4是表示HTML数据的表示例的图;

图5是表示HTML数据的验证不能进行时的表示例的图;

图6是表示图象数据的验证不能进行时的表示例的图;

图7是表示用于进行关联数据的验证的验证数据的例子的图;

图8是表示进行用于进行关联数据的验证的扩展的数据验证步骤的处理流程的图;

图9是表示接收数据高速缓冲表900的例子的图;

图10是表示包括数据验证装置的处理流程的另一个例子的图;

图11是表示导入负荷分散装置的网络构成的例子的图;

图12是表示包括数据验证装置的处理流程的例子的图;

图13是表示包括数据验证装置的网络的构成的例子的图;

图14是表示包括数据验证装置的网络的构成的例子的图;

图15是表示包括数据验证装置的网络的构成的例子的图;

图16是表示包括数据验证装置的网络的构成的例子的图。

实施例的详细说明。

下面对本发明的实施例进行说明。本实施例表示了其一个例子，本发明并不仅限于这些实施例。

（实施例1）

图1是适用本发明的一个实施例的Web系统的简图。

在图1中，100是数据要求装置。该数据要求装置是例如根据被称为HTTP（HyperText Transfer Protocol）的协议而动作的Web浏览器的软件进行工作的计算机。101是数据验证装置。102是数据提供装置。该数据提供装置是根据例如HTTP而动作的Web服务器的软件进行工作的计算机。103是连接数据要求装置和数据验证装置的网络。该网络可以是其他的装置能够连接的公开的网络，也可以是因特网。104是连接数据验证装置和数据提供装置的网络。

数据验证装置101能够在具有图2所示的一般的构成的计算机上实现。在图2中，数据验证装置101至少包含：负责进行处理的CPU等的处理部201、存储用于处理的信息的存储器（主存储部）202、硬盘等辅助存储部203、网络连接部204以及连接它们的总线等内部通信线206。如图2所示的那样，即使具有多个网络连接部204、205也没有障碍。数据验证装置的处理这样实现：在辅助存储部中所存储的程序被读入主存储器中，处理部执行所读入的程序。该程序经过通信媒体或者可移动存储媒体而读入到计算机中。

图3是表示本实施例中的各装置中的处理和各装置之间的数据交换的简要情况的图。

数据要求装置通过例如该装置的使用者进行操作，向数据验证装置进行数据的要求。

该要求根据作为要求的数据的识别符的URL（Uniform Resource Locator）来进行。要求根据HTTP被发送。

在要求接收步骤302中，数据验证装置接收来自数据要求装置的要求。由于要求包含作为要求的数据的识别符的URL或者能够判定URL的信息，因此，当接收要求时，数据验证装置能够知道所要求的数据的URL。

接着，在验证数据取得步骤303中，根据从在要求接收步骤中接收的要求而判定的URL，取得验证数据。验证数据可以是例如与上述URL相对应而将要从数据提供装置所提供的提供数据的特征值。更具体地说，特征值可以是对提供数据适用散列函数的散列值。散列函数和散列值的详细情况对本领域技术人员是公知的。

验证数据的取得能够这样进行：根据在要求接收步骤中判定的URL，来检索作为辅助存储部中的文件而把URL和散列值作为一对来存储的数据。

或者，为了取得验证数据也可以使用URL之外的信息。

或者，为了取得验证数据也可以使用对URL进行预定的处理而得到结果。

在要求接收步骤中接收的要求由包含与要求的数据相对应的辅助信息的识别符所产生。在此所谓辅助信息相当于例如用于指定要求的数据中的特定的位置的信息和对于用于生成所要求的数据的程序而指定的独立变量。在验证数据取得步骤和后述的数据验证步骤中可以忽略这样的辅助信息来进行处理。

或者，可以是来自数据库系统的验证数据的取得。

或者，设置提供验证数据的服务器装置，通过从该服务器装置取得验证数据等方法也是可以的。

在要求发送步骤 304 中，数据验证装置向数据提供装置发送提供要求。该提供要求的发送根据从要求接收步骤中接收的要求进行判定的 URL 来进行。

当数据提供装置接收提供要求时（步骤 305），向数据验证装置发送与接收的提供要求相对应的提供数据（步骤 306）。

数据验证装置在数据接收步骤 307 中接收数据提供装置发送的提供数据。

在数据验证步骤 308 中，进行接收的提供数据的验证，判断提供数据的合法性。

验证的方法可以是：例如判定对接收的数据适用散列函数而得到的散列值与在验证数据取得步骤中作为验证数据而取得的散列值是否一致。而且，当在数据接收步骤中不能取得提供数据时，在数据验证步骤中，可以作为不能确认它的合法性的情况来处理。

在数据发送步骤 309 中，对数据要求装置进行数据的发送。

是否进行数据的发送根据数据验证步骤的结果来判断。

在数据验证步骤中，当提供数据能确认它的合法性时，向数据要求装置发送从数据提供装置接收的提供数据。

在数据验证步骤中，当提供数据的合法性不能确认时，把提供数据置换为预定的数据，发送给数据要求装置。

例如，当提供数据是进行图 4 的显示的 HTML（Hyper Text Markup Language）数据时，置换成进行图 5 的显示的 HTML 数据来发送。或者，当该提供数据在数据验证步骤中合法性不能确认时，提供表示不能发送提供数据的 HTTP 状态。HTTP 状态通过状态码来表现，例如，提供状态码 404。状态码 404 是表示所要求的信息在服务器中不存在而不能发送的状态。

或者，可以切断由 HTTP 所产生的数据要求装置与验证装置的通信连接。

通过这些处理，不合法的提供数据不被发送。

前面的说明是以对 HTML 数据的验证为例进行了说明，但是，对于除此之外的种类的数据，能够进行同样的处理。

例如，当提供数据是图象数据（相当于图 4 中的 402）时，该提供数据，当在数据验证步骤中合法性不能确认时，置换为进行相当于图 6 中的 602 的显示的图

象数据来发送。

在该实施例中，验证数据是提供数据的散列值，验证这样进行：比较验证数据与根据从数据提供装置取得的提供数据而计算的散列值。但是，除此之外的实施例也是可以的。例如，对验证数据的散列值施加电子署名，在验证时同时进行电子署名的验证，由此，能够确认验证数据的散列值没有被篡改。

或者，在对散列值进行加密的基础上，作为验证数据进行登录，在数据验证步骤中，解开验证数据的密码，恢复为原来的散列值，来比较根据从数据提供装置取得的提供数据而计算的散列值。

或者，可以在验证步骤中包含对于提供数据进行预定的处理的步骤。例如，当从数据提供装置取得的提供数据是文字串时，可以比较根据把提供数据包含的预定的文字串变换为其他的预定文字串的结果而计算的散列值。在此情况下，登录在验证数据中的散列值作为根据把预定文字串变换为其他预定文字串的结果而计算的散列值。更具体地说，就是是与同一URL相对应的数据要求，当提供数据包含变化的部分时，可以包含把用表示变化部分的开始和结束的文字串围住的文字串变换为空的文字串的处理。

而且，对提供数据进行的预定的处理可以构成为根据提供数据来选择。选择的标准可以是与提供数据相对应的URL。或者，该选择的标准是提供数据的种类。

或者，取代散列值，登录提供数据的作为验证数据，可以比较在验证时所登录的提供数据与从数据提供装置取得的提供数据是否一致。

或者，在验证数据取得步骤中，可以特别规定能够取得验证数据时的处理。

当不能取得验证数据时，在数据验证步骤中，可以视为能够确认提供数据的合法性来进行处理。或者，提供数据在数据验证步骤中视为能确认它的合法性，并能够明示地指定。例如，作为验证数据，登录能够与通常的散列值区别的特定的值，在数据验证步骤中，当验证数据是该特定的值时，通过视为可以确认它的合法性来实现。

或者，当验证数据不能取得时，在数据验证步骤中，可以视为提供数据的合法性不能确认来进行处理。此时，可以不进行要求发送步骤和数据接收步骤。

在此情况下的处理为图12所示的那样。在验证数据可取得判定步骤311中，判定验证数据取得的可否，当不能取得时，进到数据验证步骤，在该步骤中，视为提供数据的正当性不能确认来进行处理。

或者，可以附加把验证结果记录在日志文件中的处理。

或者，可以根据验证结果来向预定的管理者通知验证结果的处理。特别是，当提供数据的合法性不能确认时，可以追加通过电子邮件来通知合法性确认失败的发生的处理。上述预定的管理者可以是数据验证装置的管理者。或者，上述预定的管理者可以是与合法性确认失败的数据相关而负担管理责任的管理者。可以取代电子邮件进行其他方法的通知，也可以与电子邮件一起进行其他方法的通知。

虽然对数据验证装置和数据提供装置是不同的装置的情况进行了说明，但是，在同一装置中，使实现数据验证装置的处理的程序（以下称为数据验证程序）和实现数据提供装置的处理的程序（以下称为数据提供程序）来动作也是可以的。在此情况下，数据要求装置向数据验证程序和数据提供程序工作的装置发送要求，数据验证程序接收该要求。

而且，数据验证程序向数据提供程序发送要求。

而且，数据提供程序从数据验证程序接收要求，向数据验证程序发送数据。

而且，数据验证程序从数据提供程序接收数据，向数据要求装置发送数据。

而且，数据要求装置从数据验证程序接收数据。

或者，在数据验证装置中同时执行多个OS，并且，在一个OS上执行上述说明的数据验证装置的处理，而从在其他的OS上所执行的程序来监视上述数据验证装置的处理是否正确执行。

或者，在数据验证装置中同时执行多个OS，并且，把上述说明的数据验证装置的处理分割成至少两个以上的处理，在至少两个以上的OS上进行处理。

例如，分割成进行与数据验证装置的外部进行通信的处理和包含除此之外的验证步骤的处理。在不同的OS中执行各个处理，在两OS之间各个处理关联动作，因此，能够仅进行限定的信息的交换。由此，例如，与数据验证装置的外部进行通信的处理即使经过网络而受到不正当攻击的情况下，也能防止验证步骤等进行的处理不成为攻击的对象。

或者，通过数据验证装置中的处理的并行化等，也可以实现处理的高速化。特别是，可以并行验证数据取得步骤303和从要求发送步骤304到数据接收步骤307的处理。

或者，通过进行从数据要求装置所要求的数据的预测，数据验证装置施加从

数据提供装置取得数据的处理，由此，可以实现高速化。

而且，验证数据可以由数据验证装置生成。

或者，可以设置登录在验证数据取得步骤中取得的验证数据的数据管理装置。数据管理装置进行验证数据的生成，把生成的验证数据登录到数据验证装置中。

或者，数据管理装置保存验证数据，在验证数据取得步骤中从数据管理装置取得验证数据。

或者，数据管理装置进行对数据提供装置的数据的登录。

而且，如图13所示的那样，连接数据管理装置和数据验证装置，当向数据提供装置登录数据时，通过数据验证装置进行登录。

或者，如图14所示的那样，连接数据管理装置和数据提供装置，当向数据验证装置中登录数据时，通过数据提供装置进行登录。

或者，如图15所示的那样，连接数据管理装置和网络103，通过网络向数据验证装置进行登录。在此情况下，当向数据提供装置登录数据时，通过数据验证装置进行登录。

或者，如图16所示的那样，连接数据管理装置和网络104，通过网络向数据验证装置和数据提供装置进行登录。

或者，网络103、104可以包含其他的网络设备。例如，在数据验证装置与数据要求装置之间，可以存在路由器和防火墙等设备。

而且，验证装置可以是管理数据提供装置的人进行管理的装置。或者，可以是与管理Web网站的人不同的第三者进行管理的装置。或者，可以是使用数据要求装置的人管理的装置。

而且，数据要求装置与数据验证装置进行通信的通信协议同数据验证装置与数据提供装置进行通信的通信协议是不同的。例如，前者的通信协议是通过被称为SSL（Secure Socket Layer）的方法进行加密的HTTPS的协议，后者的通信协议可以是HTTP。而且，也可以是其他的协议的组合。

而且，数据要求装置要求数据时使用的识别符与数据验证装置向数据提供装置要求数据时使用的识别符是不同的。在此情况下，在数据验证装置中，进行吸收识别符的差别的变换处理。

更具体地说，当识别符是URL时，在数据验证装置接受的要求中包含的URL

可以在数据验证装置中变换与数据提供装置的哪个URL相对应。例如，当数据要求装置要求数据时使用的URL是http://sitel/index.html，数据验证装置向数据提供装置要求数据时使用的URL是http://site2/index.html时，数据验证装置进行该URL的变换。

例如，在要求接收步骤中包含该变换处理。

或者，在要求发送步骤中包含该变换处理。

而且，把与验证数据相对应来进行管理的URL，通过与变换前后与哪个URL相对应来管理，在验证数据取得步骤中，与对应管理的URL进行整合，为此，包含变换用于验证数据取得的URL的处理。

为了对应于该变换而完成数据要求，作为数据要求装置要求数据时使用的URL的http://sitel/index.html中包含的计算机名（在此例中为site1）与数据验证装置的IP地址相对应，为此，从计算机名来解决IP地址，登录到地址解决机构中。更具体地说，例如，对于被称为DNS（Domain Name System）的结构，进行数据验证装置的IP地址和计算机名的对应的登录。同样，

http://site2/index.html中包含的计算机名（该例中为site2）与数据提供装置的IP地址相对应地进行登录。但是，数据验证装置用于与数据提供装置的通信的URL的IP地址的解决不是必须在数据要求装置中进行的，也可以在数据验证装置中进行，因此，site2的登录可以在从计算机名解决IP地址的机构中，仅登录到从限定范围的计算机能够参照的解决机构中。

更具体地说，可以仅向从连接在网络104上的装置能够参照的DNS登录数据提供装置的计算机名和IP地址的对应。或者，在数据验证装置本身中管理数据提供装置的计算机名与IP地址的对应，作为解决机构来利用。在此情况下，数据要求装置通过使用数据验证装置的计算机名的URL来进行数据的要求。而且，在数据要求装置中，不能从数据提供装置的计算机名来进行IP地址的解决，因此，指定数据提供装置的计算机名的数据要求不能进行。

或者，不进行URL的变换，进行数据要求装置、数据验证装置、数据提供装置的网络设定，以便于能够在同一URL下进行处理。更具体地说，在数据要求装置进行参照的地址解决机构中与数据验证装置的IP地址相对应地登录上述URL中包含的计算机名。而且，在数据验证装置进行参照的地址解决机构中与数据验证装置的IP地址相对应地登录上述URL中包含的计算机名，由此来实现。

而且，在需要或者不需要进行URL的变换时，连接数据要求装置和数据提供装置的网络，如图1所示的那样，通过仅经过数据验证装置所连接的构成，能够防止数据要求装置绕过数据验证装置而取得数据。

或者，不是通过物理性网络构成，而是通过防火墙等的网络设备的设定，作为逻辑的连接关系，连接数据要求装置和数据提供装置的网络必须通过数据验证装置作为中介来构成。

对于计算机名和IP地址的解决机构的细节以及网络构成的细节，本领域技术人员是公知的。

（实施例2）

HTML数据具有与成为基础的该HTML数据相关联的数据。例如，进行图4所示的显示的HTML数据具有图象数据402，作为与HTML数据相关联的数据。

在图4中，图象数据402为与HTML数据相对应的在线图象，但是，关联的数据并不仅限于在线图象，可以是任意数据。

当相对应HTML数据而存在关联数据时，在HTML数据的验证时，可以与关联数据的验证一起进行。

因此，对于任一种数据，需要哪种数据是哪个关联数据的信息。例如，验证数据包含与上述识别符相对应发送的提供数据和将要验证的关联数据的识别符，由此，能够知道所要求的数据相对应的关联数据的有无及其识别符。即，作为验证数据，与HTML数据的URL相对应，包含关联数据的URL来取得。

而且，通过包含关联数据取得步骤和关联数据验证步骤，在数据要求时，当存在与所要求的数据相对应的关联数据时，进行关联数据的验证，可以决定所要求的数据的发送的可否。

验证数据在图7中进行了具体的表示。

701是成为基础的数据的URL，702是与成为基础的URL相对应的关联数据的URL。

703是与关联数据的URL相对应的数据的散列值。

但是，作为关联数据的URL来登录预定的值时（例如NULL），703是与成为基础的数据的URL相对应的数据的散列值。

作为验证处理，对于实施例1所示的处理，扩展了数据验证步骤和数据提供步骤。

在数据验证步骤中，把图3的数据验证步骤308扩展为图8所示的。

在数据验证（2）步骤801中，与数据验证步骤308相同，进行接收的提供数据的验证。

在数据验证（2）步骤803中，如果合法性能够确认，进到步骤804，如果合法性不能确认，进到811。

在步骤804中，判定将要验证的关联数据的有无。

该步骤中的判定是判定在验证数据的关联数据中未被验证的数据是否遗留。当应当验证的关联数据遗留时，进到步骤805，当没有遗留时，进到811。

在关联数据要求发送步骤805中，在将要验证的关联数据中，从未验证中选择一个，向数据提供装置要求该数据的发送。

数据提供装置接收该要求（步骤806），发送与要求相对应的数据（步骤807）。

在关联数据接收步骤808中，从数据提供装置接收将要验证的关联数据。

在关联数据验证步骤809中，进行在关联数据接收步骤808中接收的关联数据的验证。

验证的方法可以是：判定对接收的关联数据使用散列函数而得到的散列值与验证数据取得步骤中取得的验证数据中与关联数据相对应的散列值是否一致。

在步骤810中，根据上述关联数据验证步骤的结果，当能够确认它的合法性时，即，即散列值相一致时，返回步骤804，当合法性不能被确认时，即，散列值不一致时，进到步骤811，返回步骤309。

在数据发送步骤309中，当在数据验证（2）步骤801和关联数据验证步骤809两者中它的合法性都能够确认时，向数据要求装置发送从数据提供装置接收的提供数据。

当在数据验证（2）步骤801或者关联数据验证步骤809中存在不能确认数据的合法性时，把提供数据置换为预定的数据，发送给数据要求装置。

或者，当数据验证（2）步骤801或者关联数据验证步骤809中存在不能确认数据的合法性时，与实施例1所示的相同，切断由HTTP所产生的数据要求装置与验证装置的通信的连接，或者，提供表示不能发送提供数据的HTTP的状态。

或者，关联数据中的至少一个可以是能够验证提供数据在正确的的信息。例如，更具体地说，某个提供数据的关联数据中的一个是图象数据，可以同时具有用于验证使用该图象作为关联数据的提供数据的URL的信息。

用于验证是正确的的信息并不仅限于 URL，可以是提供数据的散列值和数据尺寸以及有效期限。

或者，可以施加电子署名，表示用于验证这些提供数据是正确的的信息未被改变。

由此，进行从数据验证装置提供的数据的验证，同时，在数据要求装置中，从接收的提供数据和作为能够验证提供数据是正确的的信息的关联数据，来验证提供数据是正确的。

（实施例 3）

相对于实施例 2，表示了这样的实施例：通过在验证装置中暂时存储从数据提供装置接收的数据，来实现响应的高速化。

对于图 3 的处理流程，扩展在要求发送步骤 304、数据接收步骤 307、数据验证步骤 308 中进行的处理。

数据验证装置设有接收数据高速缓冲表 900（图 9），与识别符和接收时刻相对应地记录从数据提供装置接收的数据。

在要求发送步骤 304 中，分析在接收数据高速缓冲表 900 中是否存在将要向数据提供装置要求的数据，当不存在时或者虽然存在但该数据的接收时刻为预定时间以上的旧的时，向数据提供装置发送要求，当在接收数据高速缓冲表 900 中存在时，不发送要求，进到数据接收步骤 307。

在数据接收步骤 307 中，分析在接收数据高速缓冲表 900 中是否存在将要向数据提供装置要求的数据。

当表中不存在数据时，或者，虽然存在但该数据的接收时刻为预定时间以上的旧的时，从数据提供装置接收数据。

当在接收数据高速缓冲表 900 中存在时，不接收要求，把在接收数据高速缓冲表 900 中存在的数据交给数据验证步骤 308。

使用图 8 来说明数据验证步骤 308 中的扩展。

在数据验证（2）步骤 801 中，不进行提供数据的验证，提供数据是从数据提供装置接收的，通过验证数据能够确认合法性时，并用作为该数据的识别符的 URL 和接收时刻，在接收数据高速缓冲表 900 中登录提供数据。

在关联数据要求发送步骤 805，与要求发送步骤 304 相同，分析在接收数据高速缓冲表 900 中是否存在将要向数据提供装置要求的数据，当不存在时或者虽然

存在但该数据的接收时刻为预定时间以上的旧的时，向数据提供装置发送要求，当在接收数据高速缓冲表 900 中存在时，不发送要求，进到关联数据接收步骤 808。

在关联数据接收步骤 808 中，与数据接收步骤 307 相同，分析在接收数据高速缓冲表 900 中是否存在将要向数据提供装置要求的数据。

当表中存在数据，并且，该数据的接收时刻比预定时间新时，不向数据提供装置发送要求，把在接收数据高速缓冲表 900 中存在的数据移交给关联数据验证步骤 809。而且，在上述以外的条件下，向数据提供装置发送要求。通过不发送要求，不进行与来自数据提供装置的发送数据取得相关的处理，能够谋求处理的减轻。

在关联数据验证步骤 809 中，进行在关联数据接收步骤中取得的关联数据的验证。

关联数据是从数据提供装置接收的，当通过验证数据能够确认合法性时，并用作为该数据的识别符的 URL 和接收时刻，在接收数据高速缓冲表 900 中登录提供数据。

上述变更点之外与实施例 2 同样进行处理。

或者，当记录验证结果，一次进行与某个 URL 相对应的提供数据的验证时，在预定期间不进行对该 URL 的验证，可以利用已经进行的验证结果。

而且，当数据要求装置在要求数据时使用的识别符与数据验证装置向数据提供装置要求数据时使用的识别符不同时，在接收数据高速缓冲表 900 中，通过把与接收数据相对应的识别符与哪个识别符相对应，在进行向接收数据高速缓冲表 900 的登录、参照时，可以包含识别符的变换处理。

（实施例 4）

与实施例 1 相同，图 1 是使用本发明的一个实施例的 Web 系统的简图，图 2 是表示数据验证装置的构成的简图。

但是，本实施例中的各装置中的处理和各装置之间的交换情况为图 10 所示的那样，数据验证装置在数据接收步骤 1006 之后，进行验证数据取得步骤 1007，然后，进行数据验证步骤 1008，这点与实施例 1 不同。

在验证数据取得步骤中，与实施例 1 相同，可以从数据库取得与接收的要求相对应的验证数据。或者，可以与实施例 2、3 所示的实施例进行组合。

或者，作为另一个实施例，采取下面说明的形态。

在本实施例中，接收的提供数据是包含用于进行提供数据的验证的验证数据的数据，在验证数据取得步骤中，从提供数据取得提供数据包含的验证数据。更具体地说，提供数据是施加了电子署名的数据，在验证数据取得步骤中，从提供数据取得电子署名。

而且，在数据验证步骤中，根据作为验证数据的电子署名，进行提供数据的验证。

对于来自施加电子署名的数据的署名的取得和根据署名进行的提供数据的验证的细节，本领域技术人员是公知的。

（实施例 5）

如图 11 所示的那样，在连接数据要求装置 1100 和数据验证装置的网络之间设置负荷分散装置 1105，对于负荷分散装置，设置多个数据验证装置 1101 和与数据验证装置相连的数据提供装置 1102。

负荷分散装置当从数据要求装置接收要求时，根据预定的基准向任一个数据验证装置发送要求，而且，当从数据验证装置收取数据时，向数据要求装置传送收取的数据。

而且，对于向数据验证装置传送的要求，当从数据验证装置收取预定的数据时，根据预定的基准，向其他的数据验证装置再次传送要求。该负荷分散装置的细节本领域技术人员是公知的。

数据验证装置与实施例 1 所示的数据验证装置在以下两点上是不同的：

即，不对数据要求装置而是对负荷分散装置进行要求的接收和数据的提供。而且，在数据验证步骤中，当提供数据的合法性不能确认时，负荷分散装置向其他的数据验证装置发送进行要求的再发送的条件的数据。

具体地说，当实施例 1 所示的合法性不能确认时，在发送的数据中，可以发送与负荷分散装置的判定基准相吻合的数据。

例如，可以发送表示不能发送提供数据的 HTTP 的状态。

当合法性不能确认时，对于发送的数据应当是哪个数据的细节，对于知道负荷分散装置的细节的本领域技术人员是公知的。

（实施例 6）

对从数据提供装置向数据要求装置发送的数据被加密的实施例进行说明。在

本实施例中，以SSL所进行的加密为例进行说明，但也可以是其他方式所进行的加密。

与实施例1相同，图1是适用本发明的一个实施例的Web系统的简图，图2是表示数据验证装置的构成的简图。但是，以下内容与实施例1不同：在数据验证装置中进行与在数据发送要求之前进行的密码参数相关的处理；数据验证装置收取加密的数据，在数据验证装置中进行加码来进行验证；数据验证装置送出的数据被加密。

在SSL中，在进行加密的通信的开始之前，进行密码参数的交换。这被称为通常信号交换。在信号交换中，在数据提供装置和数据要求装置双方中生成随机数，发送给另一方。

而且，数据提供装置的公开键证明书从数据提供装置发送给数据要求装置。

而且，从数据要求装置发送成为在以后的加密中使用的计算加密键的原来的数值。该数据在用数据提供装置的公开键进行加密的状态下被发送，因此，除具有与公开键相对应的专用加密键的数据提供装置之外，以秘密的状态进行发送。

在这样进行加密的通信中，为了进行验证处理，在数据验证装置中也具有与公开键相对应的加密键，并且，保持在信号交换时所交换的密码参数，在以后的通信中，对交换的信息进行解码来进行验证。即，在数据提供装置和数据要求装置的信号交换时，数据验证装置进行两装置之间的通信的传送，但是，此时，在存储区域中保存从数据要求装置所发送的随机数和从数据提供装置所发送的随机数。而且，从数据要求装置发送给数据提供装置的加密的数值，用在数据验证装置中设置的数据传送装置的专用加密键进行解码，保存在存储区域中。从这两个随机数和解码的数值，在数据验证装置中通过由SSL规定的方法来算出在以后的通信的加密中使用的加密键。

这些值可以与识别通信的对话的对话ID相对应来保持。而且，在算出了以后通信中使用的加密键之后，加密键之外的信息可以从存储区域中丢弃。信号交换中的通信的细节、SSL的处理的细节、与对话ID的关系，对于本领域技术人员是公知的。

在数据要求装置和数据提供装置中，与数据要求装置中处理相同来进行加密键的计算，用于以后的通信的加密和解码。

在数据验证装置进行验证处理时，使用上述算出的加密键，对加密的信息进

行解码，来进行验证处理。通过对在要求接收步骤中接收的信息进行解码，来取得要求的数据的URL。在要求发送步骤中，数据验证装置向数据提供装置发送从数据要求装置接收的加密状态下的要求。

数据验证装置，在数据接收步骤中，接收数据提供装置发送的加密的提供数据。在数据验证步骤中，对接收的数据进行解码，进行验证，判断提供数据的合法性。

在数据发送步骤中，当进行数据的发送时，发送数据提供装置发送的加密的提供数据。

在此，在数据验证步骤中，当提供数据的合法性不能确认，把提供数据置换为预定的数据，而发送给数据要求装置时，或者，当发送表示不能发送提供数据的HTTP的状态时，用上述加密键对发送的数据进行加密来发送。

而且，可以组合上述各个实施例来实施。

如上述那样，通过本发明，能够防止被篡改的数据和本不应公开的数据被提供给数据要求装置。

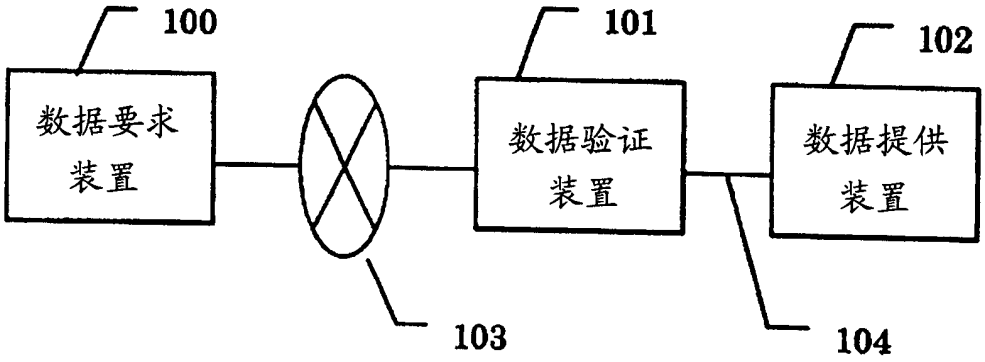

100
101
102
数据要求装置
数据验证装置
数据提供装置
103
104

图 1

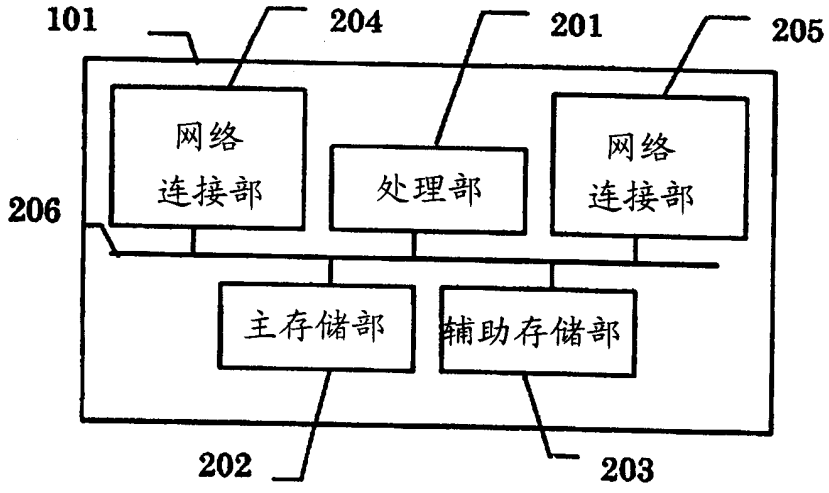

101
204
201
205
网络连接部
处理部
网络连接部
206
主存储部
辅助存储部
202
203

图 2

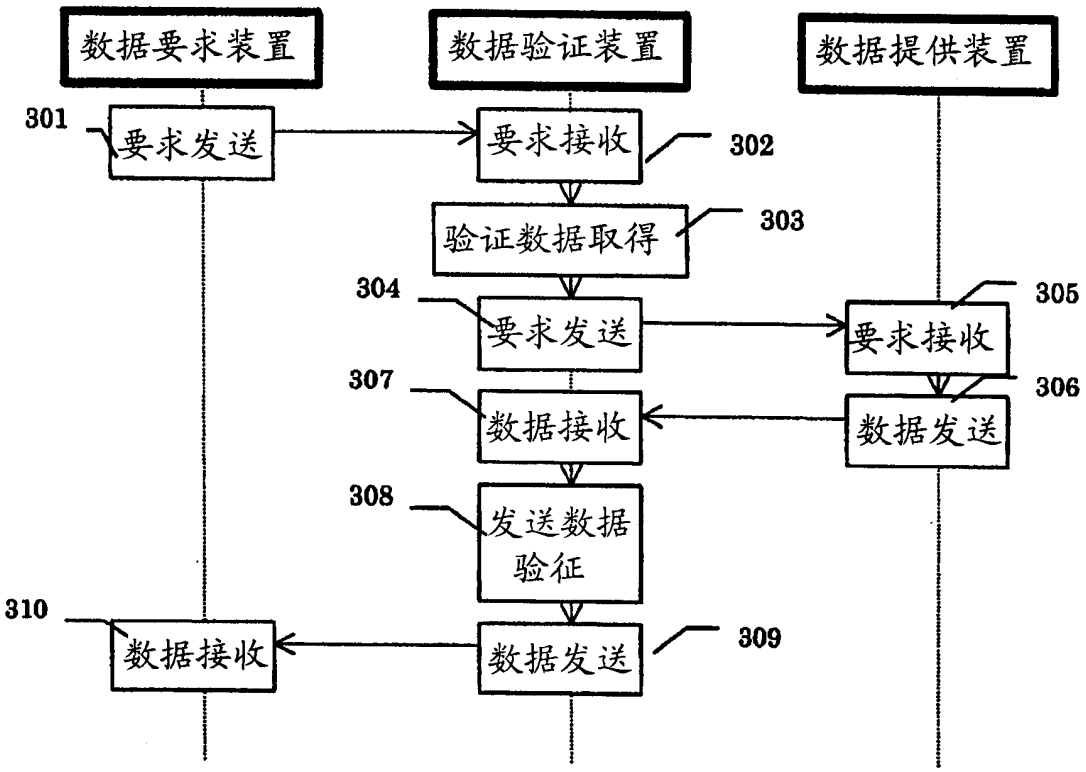

数据要求装置
数据验证装置
数据提供装置
301
要求发送
要求接收
302
验证数据取得
303
304
要求发送
要求接收
305
307
数据接收
数据发送
306
308
发送数据验征
310
数据接收
数据发送
309

图 3

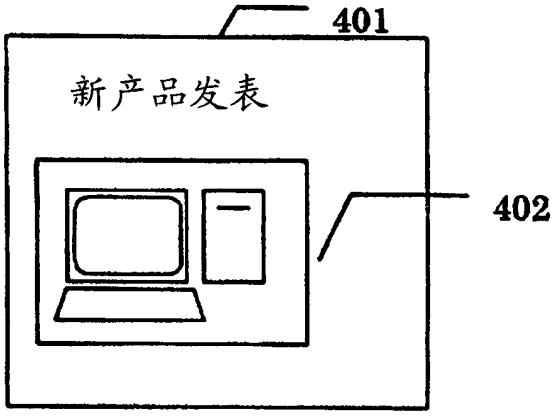
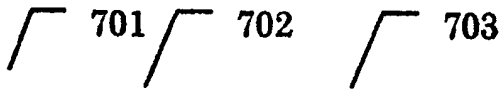

401
新产品发表
402

图 4



URL1、NULL与URL1 相对应的数据的散列值

URL1、URL2与URL2 相对应的数据的散列值

URL1、URL3与URL3 相对应的数据的散列值

URL2、NULL与URL2 相对应的数据的散列值

URL3、NULL与URL3 相对应的数据的散列值

图 7

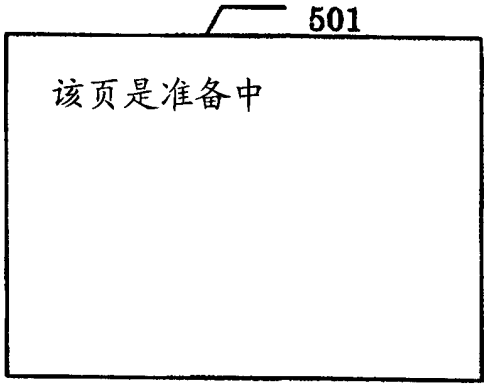


图 5

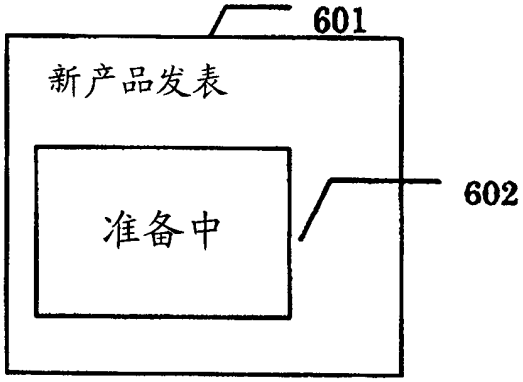


图 6

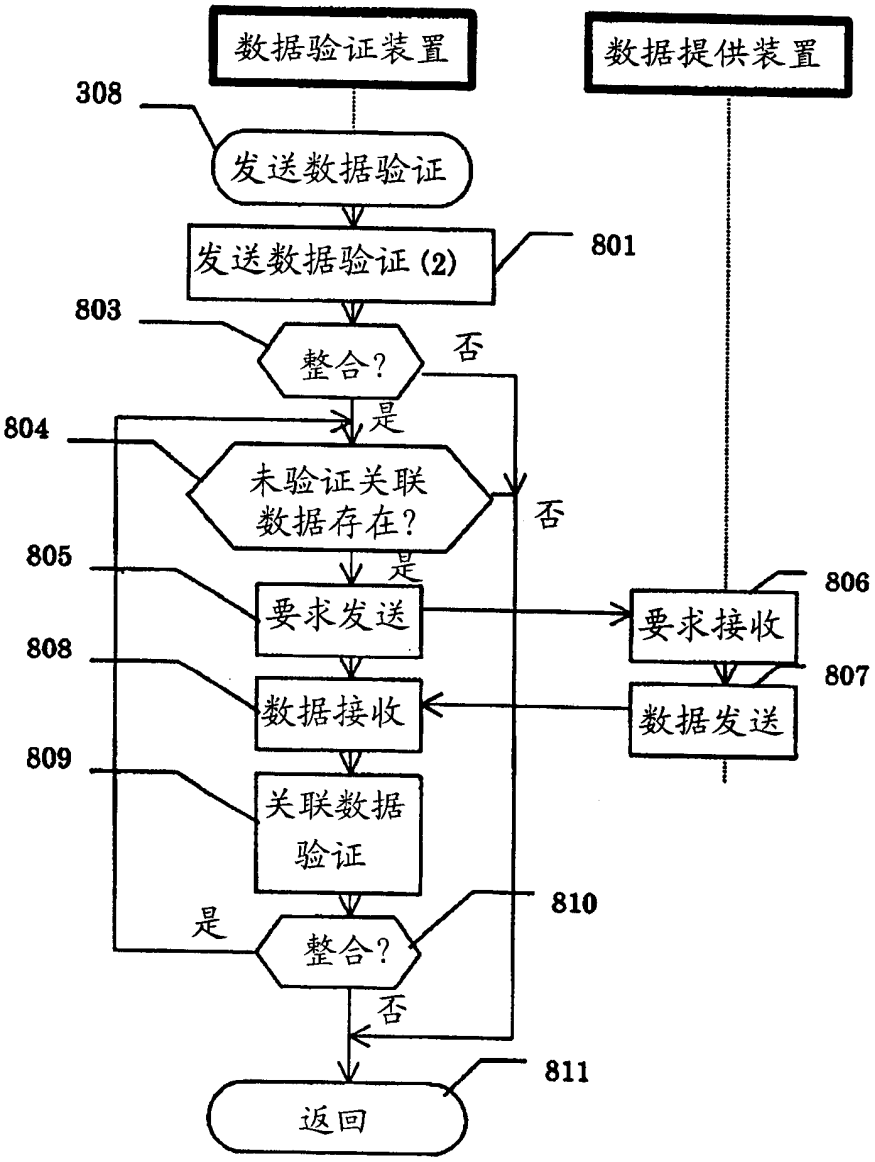

数据验证装置
数据提供装置
308
发送数据验证
发送数据验证(2)
801
803
整合?
否
是
804
未验证关联数据存在?
否
是
805
要求发送
806
要求接收
808
数据接收
807
数据发送
809
关联数据验证
是
整合?
810
否
811
返回

图 8

识别符	接收时刻	接收数据
URL1	2001/07/21 201112	与URL1 相对应的数据
URL2	2001/07/21 195438	与 URL2 相对应的数据
URL3	2001/07/21 195802	与 URL3 相对应的数据

901 902 903

图 9

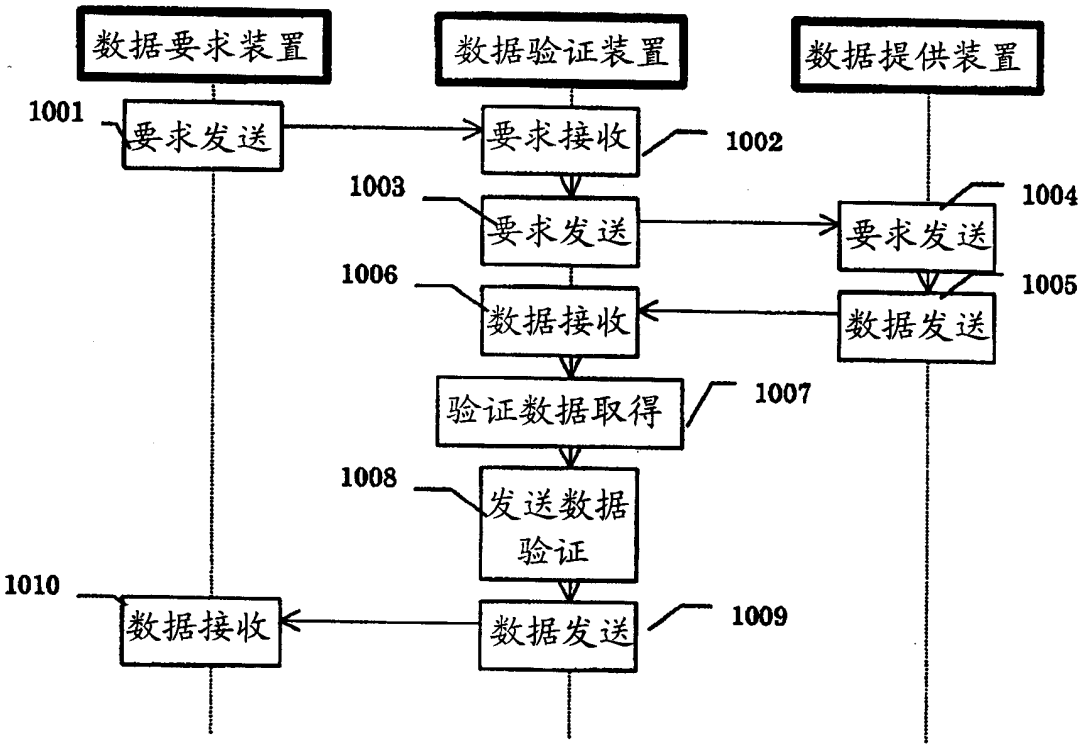


图 10

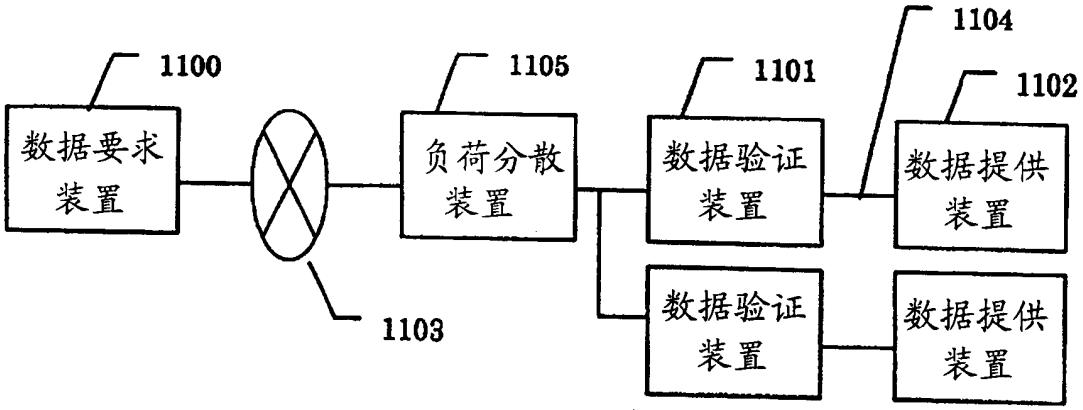

1100
数据要求装置
1103
1105
负荷分散装置
1101
数据验证装置
数据验证装置
1104
1102
数据提供装置
数据提供装置

图 11

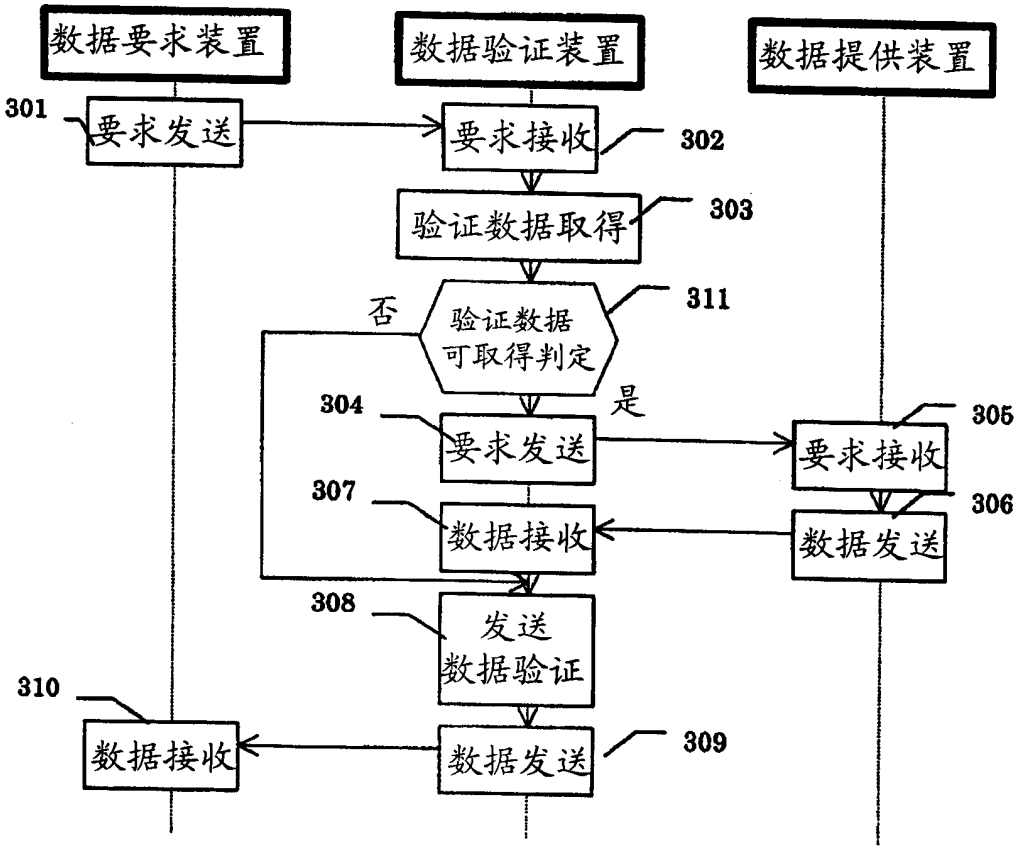

数据要求装置
数据验证装置
数据提供装置
301
要求发送
要求接收
302
验证数据取得
303
否
验证数据可取得判定
311
是
304
要求发送
305
要求接收
307
数据接收
306
数据发送
308
发送数据验证
310
数据接收
数据发送
309

图 12

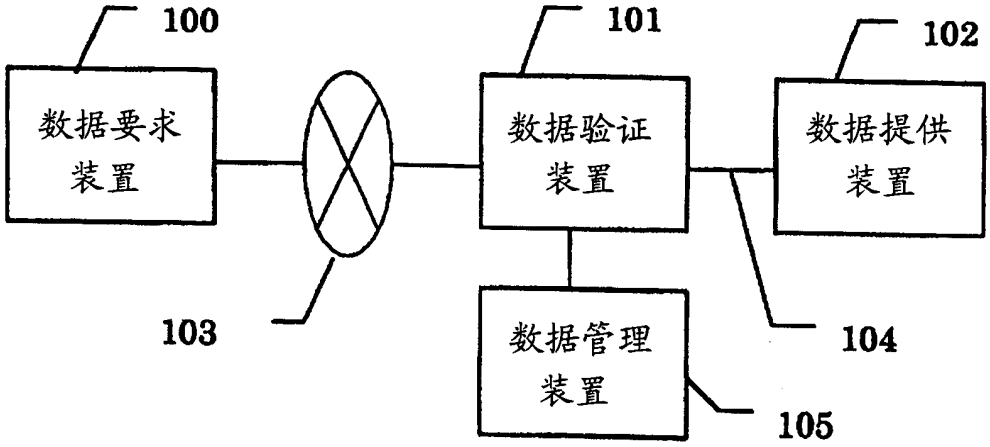

100
101
102
数据要求装置
数据验证装置
数据提供装置
103
104
数据管理装置
105

图 13

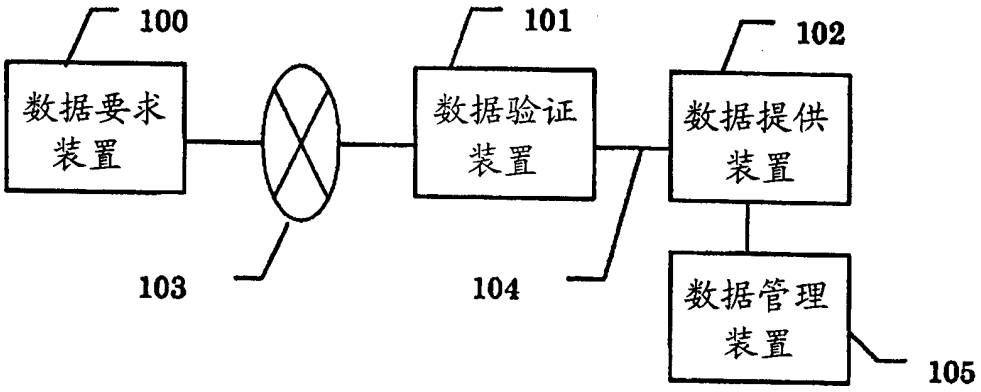

100
101
102
数据要求装置
数据验证装置
数据提供装置
103
104
数据管理装置
105

图 14

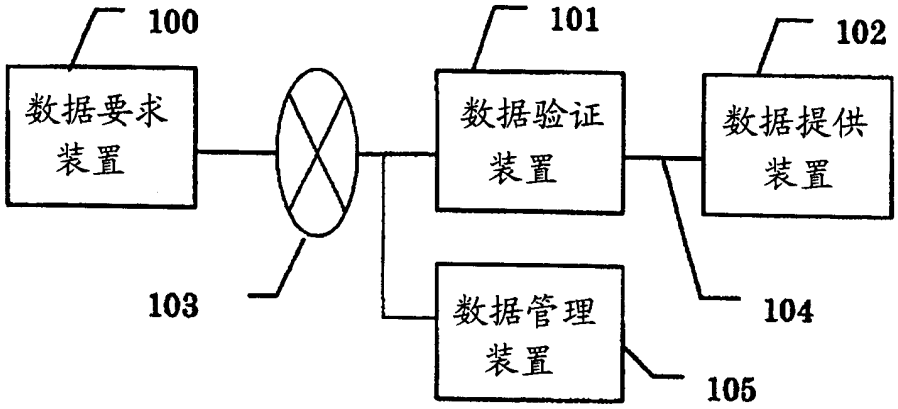

100
101
102
数据要求装置
数据验证装置
数据提供装置
103
104
数据管理装置
105

图 15

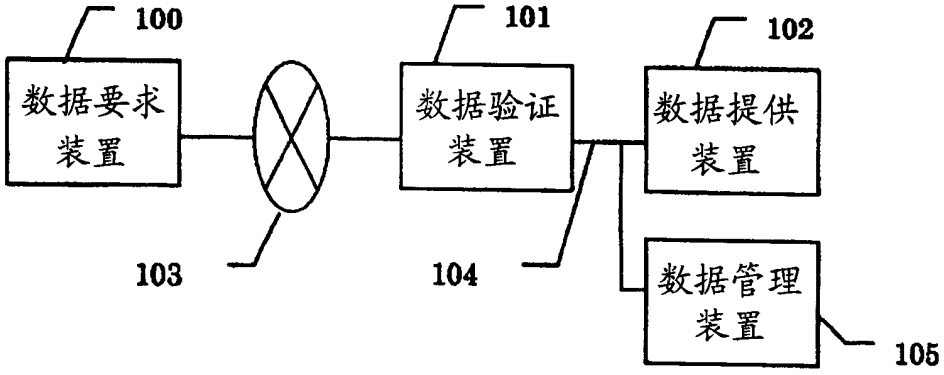

100
101
102
数据要求装置
数据验证装置
数据提供装置
103
104
数据管理装置
105

图 16