[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 29/00
G06F 13/00 G06F 9/06
H04L 12/66 H04M 11/06

[12] 发明专利申请公开说明书

[21] 申请号 03120656.5

[43] 公开日 2003 年 9 月 3 日

[11] 公开号 CN 1440170A

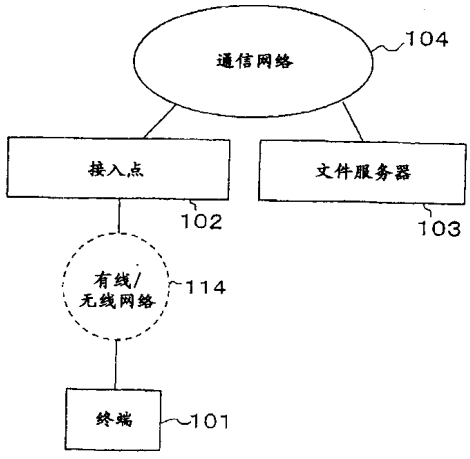
[22] 申请日 2003.2.8 [21] 申请号 03120656.5
[30] 优先权
[32] 2002. 2. 8 [33] JP [31] 031872/2002
[71] 申请人 株式会社东芝
地址 日本东京都
[72] 发明人 利光清 高木雅裕
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 王以平

权利要求书 3 页 说明书 13 页 附图 9 页

[54] 发明名称 通信系统、终端设备、接入点装置及安全措施文件的下载方法

[57] 摘要

一种通信系统，由管理安全措施文件的文件服务器和从文件服务器下载安全措施文件后施行安全措施的终端构成。 终端基于现在可利用的通信频带，选择安全措施文件的下载方针。



ISSN1008-4274

1. 一种通信系统，包括:

管理安全措施文件的文件服务器；和

从上述文件服务器下载上述安全措施文件后施行安全措施的终端，

上述终端基于现在可利用的通信频带，选择上述安全措施文件的下载方针。

2. 如权利要求1所述的通信系统，其中上述终端

在通信频带处于规定的阈值以上的情况下，在进行其他通信之前下载上述安全措施文件，

在通信频带处于规定的阈值以下的情况下，一边进行其他通信，一边下载上述安全措施文件。

3. 如权利要求2所述的通信系统，进一步包括:

进行通信数据的安全检验和措施的屏蔽服务器，

其中，

在上述终端一边进行其他通信一边下载上述安全措施文件的期间，经由上述屏蔽服务器进行上述其他通信。

4. 一种通信系统，包括:

管理安全措施文件的文件服务器;

指令安全措施的指令服务器；和

基于上述指令服务器的指令，从上述文件服务器下载上述安全措施文件后施行安全措施的终端，

上述终端调查现在可利用的通信频带，传达给上述指令服务器，上述指令服务器基于上述通信频带，向上述终端指令上述安全措施文件的下载方针。

5. 如权利要求4所述的通信系统，其中，

上述指令服务器和上述文件服务器由一台计算机构成。

6. 如权利要求4所述的通信系统，其中，

上述指令服务器是上述终端与通信网络连接时的连接点。

7. 如权利要求4所述的通信系统，其中上述终端

在通信频带处于规定的阈值以上的情况下，在进行其他通信之前下载上述安全措施文件，

在通信频带处于规定的阈值以下的情况下，一边进行其他通信，一边下载上述安全措施文件。

8. 如权利要求7所述的通信系统，进一步包括:

进行通信数据的安全检验和措施的屏蔽服务器，

其中，

在上述终端一边进行其他通信一边下载上述安全措施文件的期间，经由上述屏蔽服务器进行上述其他通信。

9. 一种安全措施文件的下载方法，其中通信系统包括：管理安全措施文件的文件服务器;从上述文件服务器下载上述安全措施文件后施行安全措施的终端；以及连接上述文件服务器与上述终端的通信网络，所述下载方法下载上述通信系统的上述终端使用的安全措施文件，包括:

调查现在可利用的通信频带的通信频带检验步骤;

在通信频带处于规定的阈值以上的情况下，在进行其他通信之前下载上述安全措施文件的即时更新步骤；以及

在通信频带处于规定的阈值以下的情况下，一边进行其他通信，一边下载上述安全措施文件的后台更新步骤。

10. 如权利要求9所述的安全措施文件的下载方法，其中

上述通信系统包括与上述通信网络连接的进行通信数据的安全检验和措施的屏蔽服务器，

在上述后台更新步骤运行时进行的其他通信经由上述屏蔽服务器进行。

11. 一种终端设备，包括:

与通信网络连接的连接装置;

确立通过与管理安全文件的文件服务器间的通信网络的通信的通信确立装置;

调查现在可利用的通信频带的频带调查装置；和

基于由上述频带调查装置得到的可利用的通信频带，决定上述安全措施文件的下载方针的方针决定装置。

12. 如权利要求11所述的终端设备，其中上述方针决定装置

在通信频带处于规定的阈值以上的情况下，就选择在进行其他通信之前下载上述安全措施文件的即时更新方针，

在通信频带处于规定的阈值以下的情况下，就选择一边进行其他通信，一边下载上述安全措施文件的后台更新方针。

13. 一种与通信网络连接的成为与上述通信网络连接的终端连接点的接入点装置，包括:

确立与上述终端之间的通信的通信确立装置;

媒介上述终端与上述通信网络间的通信的媒介装置;

上述终端调查现在可利用的通信频带的频带调查装置;

基于由上述频带调查装置得到的可利用的通信频带，向上述终端指示的、根据与上述网络连接的管理安全措施文件的文件服务器决定安全措施文件的下载方针的方针决定装置；和

向上述终端指示上述已决定的下载方针的指示装置。

14. 如权利要求13所述的接入点装置，其中上述方针决定装置

在通信频带处于规定的阈值以上的情况下，就选择在进行其他通信之前下载上述安全措施文件的即时更新方针，

在通信频带处于规定的阈值以下的情况下，就选择一边进行其他通信，一边下载上述安全措施文件的后台更新方针。

通信系统、终端设备、接入点装置及安全措施文件的下载方法

前后参照的相关申请

本申请基于在前的日本专利申请No.2002-31872，其申请日是2002年2月8日，并要求其优先权，其全部内容作为参考包含在本文中。

技术领域

本发明涉及通信系统中的安全措施。

背景技术

伴随着近年的网络技术的发展，多数PC（Personal Computer 即，个人计算机）都与网络连接。随之，计算机病毒的侵害也增大，安全措施变得很重要。

作为PC的安全措施，较多的情况是在终端安装反病毒程序等的安全措施软件。此外，修正OS（Operating System 即，操作系统）和应用程序中的不当之处的安全补丁等在PC的安全措施中也是不可缺少的。

日本专利公开公报：特开2001－159975号公报公开了一种病毒措施方法，该方法是定期运行反病毒程序，其版本若不是最新的，就进行反病毒程序本身的更新。以在PC上工作的反病毒程序中的一个为例，在网络连接时，终端运行自动更新程序，向颁布数据文件的服务器访问，以取得最新版的数据文件。

反病毒程序的规模和同程序使用的数据文件的更新差分的数据量存在增大的倾向。在PC与有线LAN连接的情况下，因为能确保充分的通信频带，所以更新处理所花费的时间很少就足够了。

因而，在用户开始通信之前，能几乎没有压力地运行安全措施软件的更新处理。

但是，在用无线LAN和携带式电话机等进行无线通信的情况和利用拨号进行有线通信的情况下，未必能常常确保充分的用于进行安全措施软件更新处理的通信频带。在通信频带不充分的状态下的安全措施软件的更新处理就需要时间，用户在等待处理结果时感觉焦躁。

作为解决该问题的方法，在日本专利公开公报：特开2001－256045号公报

公开的方法中，终端不施行经由安全服务器通信以外的安全措施。取而代之，安全服务器解析向终端发送的信息包，进行病毒检验和去除。确实，该方法不需要终端侧的更新处理，也能回避上述通信频带引起的问题。

但是，由于该方法安全服务器的负担大，因此，在终端数量增加的情况下，赶不上安全服务器自身的处理能力，而实质上有可利用的通信频带变窄的可能性。此外，也有因所谓的DoS（Denial of Service 即，拒绝服务）攻击等安全服务器耐不住负载而停止功能的情况下通信被切断的危险性。

从而期望不仅安全服务器而且各终端上也能进行安全措施。

发明内容

本发明的目的是提供一种安全措施方法和系统，其能不损伤用户的舒适性，用根据通信频带的最佳方法进行安装在PC和携带式电话机等终端上的安全措施软件和数据文件的更新。

本发明的通信系统的特征在于如下构成，包括：管理安全措施文件的文件服务器；从上述文件服务器下载上述安全措施文件后施行安全措施的终端，上述终端基于现在可利用的通信频带，选择上述安全措施文件的下载方针。

此外，本发明的通信系统的特征在于如下构成，包括：管理安全措施文件的文件服务器；向安全措施发出指令的指令服务器；基于上述指令服务器的指令，从上述文件服务器下载上述安全措施文件后施行安全措施的终端，上述终端调查现在可利用的通信频带，传达给上述指令服务器，上述指令服务器基于上述通信频带，向上述终端发出上述安全措施文件的下载方针的指令。

另外，本发明的安全措施文件的下载方法的特征在于，一种通信系统包括：管理安全措施文件的文件服务器；从上述文件服务器下载上述安全措施文件后进行安全措施的终端；以及连接上述文件服务器和上述终端的通信网络，在下载上述通信系统的上述终端使用的安全措施文件的方法中，包括下述步骤：调查现在可利用的通信频带的通信频带检验步骤；通信频带处于规定的阈值以上的情况下，在进行其他通信之前下载上述安全措施文件的即时更新步骤；通信频带处于规定的阈值以下的情况下，一边进行其他通信，一边下载上述安全措施文件的后台更新步骤。

另外，本发明的终端设备的特征在于，包括：与通信网络连接的连接装置；确立通过与管理安全文件的文件服务器间的通信网络进行通信的通信确立装置；调

查现在可利用的通信频带的频带调查装置；基于由上述频带调查装置得到的可利用的通信频带，决定上述安全措施文件的下载方针的方针决定装置。

此外，本发明的接入点装置的特征在于，该接入点与通信网络连接，成为与上述通信网络连接的终端的连接点，其中包括：确立与上述终端间的通信的通信确立装置；媒介上述终端与上述通信网络间的通信的媒介装置；上述终端调查现在可利用的通信频带的频带调查装置；基于由上述频带调查装置得到的可利用的通信频带，向上述终端指示的、根据与上述网络连接的管理安全措施文件的文件服务器决定安全措施文件的下载方针的方针决定装置；然后，向上述终端指示上述已决定的下载方针的指示装置。

附图说明

图1是说明第一、第二、第三实施例涉及的通信系统的结构的图。

图2是第一实施例涉及的通信系统的终端中的模式文件更新处理的流程图。

图3是说明用于其他程序的频带和用于更新处理的频带根据频带控制而变动的情况的图。

图4是第二实施例涉及的通信系统的终端中的模式文件更新处理的流程图。

图5是第三实施例涉及的通信系统的终端中的模式文件更新处理的流程图。

图6是说明第三实施例涉及的通信系统中的终端与文件服务器间的通信的图。

图7是说明第四实施例涉及的通信系统的结构的图。

图8是说明第四实施例涉及的通信系统中的经由了屏蔽服务器的终端与外部服务器的通信状态的图。

图9是第四实施例涉及的通信系统的终端中模式文件更新处理的流程图。

具体实施方式

（第一实施例）

图1是本发明的第一实施例涉及的通信系统的概略结构的说明图。

本实施例涉及的通信系统由下述装置构成：用户使用的终端101；终端101通过有线或无线网络进行通信的接入点102；向终端101提供安全措施软件的数据文件等的文件服务器103；连接接入点102与文件服务器103间的通信网络104。

终端101是能运行用于施行安全措施的程序，能用有线或无线进行通信的计算机。终端101也可以是台式PC、笔记本型PC、PDA等的携带式终端、或携带式

电话机。

在终端101上，在终端101购买时预先安装施行计算机病毒（以下称作“病毒”）措施的反病毒程序作为安全措施软件。反病毒程序基于存储在病毒措施数据文件（以下称作“模式文件”）中的数据，发现并去除即将入侵或已入侵到计算机的病毒。终端101进行包含在反病毒程序中的模式文件的更新处理，利用将模式文件更新成最新的文件，就能对应最新的病毒。

接入点102用有线或无线进行与终端101的通信。终端101与网络上其他计算机的通信经由接入点102进行。接入点102若在LAN环境下就相当于网关服务器和路由器，若是提供者，就相当于提供者一侧的调制解调器和网关服务器及认证服务器。此外，接入点102在终端101是携带式电话机的情况下相当于基地台。

文件服务器103存储最新的模式文件等。在文件服务器103中，更新服务器程序进行工作，它根据来自终端101的请求，提供最新的模式文件的版本号等信息和将最新的模式文件向终端101发送的远程服务。

终端101在其出厂时（或购买时）安装的模式文件中，由于不能对应最新的病毒，因此必须再三进行模式文件的更新。

图2是说明模式文件的更新处理的流程图。该处理由终端101运行。

在模式文件的更新处理之前，首先，终端101确立与接入点102间的通信（步骤S1）。这个处理是为了进行IP地址的分配等的处理，让该通信按TCP／IP标准进行通信。

若终端101与接入点102间的通信已确立，终端101就抑制由反病毒程序以外的其他程序的通信的开始，预防更新处理中的病毒感染。而且，该抑制处理不是必须的。

然后，终端101向文件服务器103请求最新的模式文件的版本号。终端101将现有的模式文件的版本号与存在于文件服务器103中的最新的模式文件的版本号进行比较（步骤S2）。

两者版本一致的情况下，由于终端101现有的模式文件是最新版，因此不需要更新处理。从而处理进入到步骤S3，开始由上述反病毒程序以外的其他程序的通信。对于文件服务器103中的模式文件的版本比终端101中现有的模式文件的版本旧的情况也一样。

在文件服务器103中存在比终端101现有的模式文件新的模式文件的情况下

，终端101对用户提示模式文件的更新处理方针，要求用户选择（步骤S4）。在模式文件的更新处理方针中，提出更新模式文件的时期或方式，例如，至少有“立即更新”、“后台更新”、“不更新”3种。

即使在模式文件的更新上需要时间，但在用户希望优先进行安全措施时，在步骤S4中，该用户可以选择“立即更新”。该情况下，即时进行更新处理（步骤S5）。由于直到更新完了的期间，其他通信全部被中断，因此即使对于旧的模式文件中不能覆盖的新种病毒在网络上蔓延的状况，也能预防终端101的病毒感染。步骤S5的即时更新处理包括从文件服务器103下载最新的模式文件的步骤S51和更新终端101内现有的模式文件成为下载下来的模式文件的步骤S52，在这些处理之后，在步骤S53允许和开始进行由其他程序通信。

另一方面，在用户希望直接开始通信时，该用户可以在步骤S4中选择“不更新”。该情况下，处理进入步骤S3，终端101中即时地允许由其他程序通信。在不能确保充分的安全的情况下，例如仅发送一份邮件等通信时间极短且不容易发生安全问题的情况下，该选择有效。

此外，想直接开始通信但也想确保安全的用户可以在步骤S4中选择“后台更新”。该情况下，进入后台更新处理（步骤S6），同时，即时地允许由其他程序通信。不能确保模式文件更新中的安全，但能确保更新后的安全，多数情况能确保充分的安全。倘若，用户想在模式文件更新完了之前结束通信的情况下，就在画面上显示在模式文件更新完了之后自动地使通信完了的意思，继续进行更新处理。

在步骤S61，后台更新处理一开始，终端101与接入点102间的全部通信频带就被模式文件的更新处理占用了，由终端101中的其他程序通信的速度就降低了，损伤了用户的舒适性。因此，进行频带控制，使模式文件更新处理占用通信频带的一部分，剩余的通信频带为由其他程序通信而开放。再者，所谓“通信频带”，就是在通过连接终端101与接入点102间的有线或无线网络114（参照图1）的通信中，终端101所使用的通信频带。此外，通信频带（宽度）的宽窄与通信速度的高低对应。即，若通信频带宽，由于单位时间内能传输的数据量进一步增加，因此通信速度就高。

在步骤S61中，例如，如图3所示，也可以自动地控制模式文件更新处理占用的通信频带按照由其他程序通信利用的频带在全部通信频带中占用的比例（频

带利用率）来变化。具体地说，在模式文件的下载期间监控在用于由其他程序通信上确保的频带的利用率。该利用率低于第一规定阈值的情况下，暂时增加分配到用于模式文件更新处理的通信频带。但是，必须确保用于由其他程序通信的下限频带。反之，在利用率高于第二规定阈值（比第一规定阈值大的值）的情况下，就减少分配到用于模式文件更新处理的通信频带。但是，必须确保分配到用于模式文件更新处理的下限频带。

再者，通信频带控制通过终端101与模式文件的供给源文件服务器103的协调工作进行。例如，终端101定期地向文件服务器103通知表示分配到模式文件更新处理的通信频带的信息。文件服务器103基于通知到的通信频带信息，调整发送到终端101的信息包的量。

此外，根据连接终端101与接入点102间的网络114中的通信方式而通信频带控制的方法不同。例如，网络114的通信媒体是无线，采用TDMA（Time Division Multiple Access 即，时分多址）方式的无线通信的情况下，就可以利用控制分配到用于模式文件更新处理的槽数和分配到用于由其他程序通信的槽数来进行无线区间的频带控制。其结果，从文件服务器103发送的单位时间左右的信息包量被调整。

或者，在采用FDMA（Frequency Division Multiple Access即，频分多址）方式和CDMA（Code Division Multiple Access 即，码分多址）方式的无线通信的情况下，通过控制分配到用于模式文件更新处理的信道数（若FDMA就是频带数，若CDMA就是代码数）来实现相同的通信频带控制。

此外，在采用CSMA（Carrier Sense Multiple Access 即，载波侦听多址）方式作为无线区间通信方式的情况下，利用控制对用于模式文件更新处理的数据和用于其他程序的数据的事后处理的优先级，也能实现相同的通信频带控制。

再者，文件服务器103发送的频带控制不限于上述方法，什么样的方法都可以。

此外，本实施例说明了按TCP／IP标准通信被确定后进行模式文件更新的内容，但TCP／IP标准不是必须的。例如，在将接入点102和文件服务器103结合成一个装置的结构中，也可以在确立TCP／IP通信的中途阶段进行模式文件更新处理。

根据以上说明的本发明的第一实施例，假设模式文件的更新花费了时间，

或即使发生了不能充分确保安全的状况，由于用户预先同意这样做，因此也不损伤用户的舒适性。在由后台进行模式文件的更新的情况下，因为仅使用通信频带的一部分进行，所以能不损伤用户的舒适性而实施安全措施。

再者，在向文件服务器106询问模式文件的版本之际，文件服务器106将最新的模式文件的文件大小通知给终端101，终端101从该文件大小和通信速度计算并提示该模式文件传输需要的时间，也可以作为用户在决定模式文件的更新处理方针时的一个帮助。

（第二实施例）

由于本发明的第二实施例涉及的通信系统的结构与第一实施例大致相同，因此只说明不同点。与第一实施例不同之处是模式文件的更新处理，不依照来自用户的指示而自动地决定模式文件的更新处理方针。

图4是说明本实施例中的模式文件更新处理的流程图。

确立终端101与接入点102的通信，终端101对文件服务器103进行访问，直到确认最新的模式文件的版本号的处理（步骤S1，S2）与第一实施例相同。

终端101的模式文件比文件服务器103的模式文件版本旧的情况下，终端101就调查与接入点102间的通信速度。通信速度的值也可以实际计测，也可以用已知的值。在步骤S4中，根据通信速度的值决定模式文件更新处理方针。

通信速度超过规定阈值的情况下，因为已知在模式文件的更新中能用充分的通信频带进行通信，所以就进行即时更新处理（步骤S5）。

通信速度低于规定阈值的情况下，因为已知在模式文件的更新中通信频带不充分，所以就进行后台更新处理（步骤S6）。再者，即使在通信速度低于阈值的情况下，若最新模式文件的文件大小极小，就进行即时更新处理也可以。

再者，本实施例应该根据终端101与接入点102间的通信速度自动地决定模式文件更新处理方针，但也可以构成为在显示了模式文件的更新中必要的估计时间后，象第一实施例那样，用户能选择模式文件更新处理方针。此外，也可以基于用户预先设定的阈值自动地决定更新处理方针。

根据本实施例，因为终端101根据现在可利用的通信速度自动地决定模式文件更新处理方针，所以就不要用户操作，不仅得到与第一实施例相同的效果，而且也能提高操作性。

（第三实施例）

因为本发明的第三实施例涉及的通信系统的结构与第二实施例大致相同，所以只说明不同点。第三实施例与第二实施例的不同点是按模式文件的版本和重要性详细地区分情况来决定模式文件的更新处理方针。

图5是说明本实施例中的模式文件更新处理的流程图。

直到确立终端101与接入点102的通信的处理（步骤S1～S2）与第一和第二实施例相同。

在终端101与文件服务器103间按照如图6所示那样的报文顺序进行模式文件的更新。

终端101对接入点103进行访问，请求最新模式文件的信息M1。该信息M1包括最新模式文件的版本号、重要性、最近的高重要性版本号。所谓重要性的参数是在文件服务器103上安装模式文件的网络管理者等每个模式文件设定一个的参数，例如，象为了对应极恶性的病毒而释放的模式文件那样，打算在各终端中直接使之更新的，就较高地设定重要性，对它以外的就较低地设定重要性。重要性的阶段是几阶段为可以，但在此假定二阶段（高阶段或低阶段）。此外，重要性和最近的高重要性的版本号准备与模式文件同名而扩展名不同的重要性文件，通过在其文件中记述而进行，但不限于此。

如图6所示，文件服务器103根据来自终端101的模式文件的信息M1的请求，回答表示模式文件的最新版本号（图6的VERSION字段）、模式文件的重要性（URGENT－LEVEL字段）、和最近的高重要性的版本号（CRITICAL－VERSION字段）的报文M2。

在终端101现有的模式文件比文件服务器103正在颁布的模式文件旧的情况下，就必须要进行模式文件的更新。终端101调查与接入点102间的通信速度，将该2个阈值与T1和T2（T1>T2）比较，选择更新处理方针（步骤S4）。

在终端101与接入点102间的通信速度超过阈值T1的情况下，终端101就选择即时更新处理（步骤S7）。

在终端101与接入点102的通信速度低于阈值T2的情况下，终端101就选择后台更新处理（步骤S8）。再者，在该步骤S8中，与第二实施例一样，不损伤用户的舒适性地进行频带控制。此外，即使在通信速度低于阈值T2的情况下，若最新模式文件的文件大小极小，就进行即时更新处理也可以。

在终端101与接入点102间的通信速度在阈值T2以上、阈值T1以下的情况下，

终端101就基于最近的高重要性的版本号进行情况划分（步骤S5）。即，在终端101现有的模式文件的版本号比最近的高重要性的版本号小的情况下，因为已知不能进行按重要性高的模式文件的更新，所以终端101就选择即时更新处理（步骤S7）。

在终端101现有的模式文件的版本号比最近的高重要性版本号大的情况下，终端101就进一步按最新的模式文件的重要性进行情况划分（步骤S6）。因为最新模式文件的重要性高时感染病毒的危险性高，所以终端101就选择即时更新处理（步骤S7）。因为模式文件的重要性低时感染病毒的危险性没有那么高，所以终端101就选择后台更新处理（步骤S8）。该情况下也与上述一样，进行频带控制而不损伤用户的舒适性。此外，即使在模式文件的重要性低的情况，若最新模式文件的文件大小极小，就进行即时更新处理也可以。

本实施例中，终端101调查通信频带，但也可以由接入点102调查通信频带后传达给终端101。

本实施例中，自动地选择更新处理方针，但最好也预备在向高级者显示了从文件服务器103得到的信息后用户能选择的方式和基于用户决定了的阈值自动地选择的方式。

此外，因为能向用户传达模式文件更新过程中的状况和不损伤用户的舒适性，所以很好。

根据本实施例，因为基于比模式文件的重要性更详细的信息决定模式文件更新处理方针，所以能不损伤用户的舒适性而且进行安全措施。

（第四实施例）

图7是说明本发明的第四实施例涉及的通信系统的结构的图。

本实施例涉及的通信系统是在图1示出的结构中加上屏蔽服务器105和外部服务器106而构成。

因为本实施例涉及的通信系统与第二实施例的通信系统结构相似，所以只说明不同部分。

屏蔽服务器105是解析输入到的通信信息包，去除病毒等后输出的程序进行工作的服务器。

外部服务器106是例如象HTTP服务器和FTP服务器等这样地与终端101进行通信的任意计算机，但假设是通过破坏操作试着对终端101不正当访问的计算机

的情况。

以下，参照图8简单地说明屏蔽服务器105的工作。图8示出终端101和屏蔽服务器105及外部服务器106间的信息包的流程。

终端101经由屏蔽服务器105与外部服务器106通信。一般地，因为从终端101向外部服务器105发送的信息包不受终端101自身的安全的影响，所以，能不经由屏蔽服务器105而直接发送到外部服务器703，或由屏蔽服务器105与普通的Proxy服务器和路由器同样地进行简单的中继。

对此，从外部服务器106向终端101发送的信息包有影响终端101安全的可能性。因此，屏蔽服务器105一旦接收该发送信息包，就解析是否包含有病毒等有害的数据。然后，屏蔽服务器105从发送信息包去除有害数据，发送到终端101，或废弃该信息包本身。这样，就从屏蔽服务器向终端101仅发送安全的发送信息包。

最好构成为能由用户选择终端101与外部服务器106间的通信是否经由屏蔽服务器105。经由屏蔽服务器105的通信中，一旦由屏蔽服务器105接收从外部的计算机向终端101发送的全部的信息包，就去除病毒等后再向终端101发送。

在终端101与屏蔽服务器105间的理论上的通信路径的结构中能使用实现MobileIP（参照IETF RFC2002）等的移动通过性的技术。通过使用MobileIP，容易实现所说的从终端101发向外部服务器106的信息包不经由屏蔽服务器105而直接到达，但从外部服务器106发向终端101的信息包经由屏蔽服务器105的上述的流程控制。

图9是说明本实施例涉及的模式文件更新处理的流程图。

本实施例与上述的第一至第三实施例的不同点是支持经由屏蔽服务器105的通信这点。

与第二实施例一样，终端101确立与接入点102间的通信（步骤S1），终端101调查自身现有的模式文件是否是最新版本（步骤S2）。然后，在模式文件不是最新的情况下，终端101就调查与接入点102间的通信速度，决定模式文件的更新处理方针。

在模式文件是最新的情况下就不需要模式文件更新处理。但是，也可以考虑在需要极高安全度的情况下，就进行经由屏蔽服务器105的通信。因此，终端101显示用户能选择屏蔽服务器使用的有无这样的规定的选择画面（步骤S3）。

在该步骤S3中，由用户选择了指示使用屏蔽服务器的项的情况下，终端101就开始进行经由屏蔽服务器105的通信（步骤S4），选择了指示不使用屏蔽服务器的项，终端101就进行不经由屏蔽服务器105的正常的通信（步骤S5）。

在终端101内的模式文件不是最新的情况下，就必须要更新模式文件。因此，终端101调查与接入点102间的通信速度（步骤S6）。

通信速度超过规定的阈值的情况，终端101就进行即时更新处理（步骤S7），模式文件的更新完了之后开始由其他程序通信。

通信速度低于规定的阈值的情况，终端101就显示用于用户选择屏蔽服务器105使用的有无的上述选择画面（步骤S8）。与上述一样，由用户指示了使用屏蔽服务器的情况下，终端101就进行后台更新处理，按经由屏蔽服务器105进行在模式文件更新中进行的其他通信（步骤S9）。再者，即使在通信速度低于阈值的情况下，若最新模式文件的文件大小极小，就进行即时更新处理构成为。

另一方面，由用户指示了不使用屏蔽服务器的情况下，为了确保安全，终端101就进行即时更新处理（步骤S7），在模式文件的更新完了后开始由其他程序通信。

再者，本实施例中，在通信速度在规定的阈值以下的情况下，让用户选择屏蔽服务器105使用的有无，但也可以不让用户选择而强制地使用。此外，也可以按模式文件的重要性自动地决定屏蔽服务器105使用的有无，在重要性低时不让使用屏蔽服务器105而进行后台更新处理。

此外，在使用屏蔽服务器105时，发送到终端101的全部信息包成为解析对象，但也可以仅解析其特定协议（例如，POP、IMAP。SMTP等，即与邮件相关）的信息包。

此外，终端101与屏蔽服务器105间的理论上的通信路径当然也可以是物理性的连接。例如，也可以使接入点102上具有屏蔽服务器105的功能。

根据本实施例，即使在模式文件的更新上花费时间的情况下，也能直接地边维持安全边进行通信，能不损伤用户的舒适性而实现安全的通信。

在第一至第四实施例中，作为由终端101进行模式文件是否更新的判断和模式文件更新处理方针的决定的方法进行了说明，但也可以由文件服务器103或接入点102决定这些，向终端101发指令。象这样地，利用由终端101以外的共用服务器等决定处理方针，能不依从于用户而均一地保证终端101的安全。

该情况下，在第一至第四实施例中，也可以代替终端101进行调查这些模式文件的版本的处理，将终端101现有的模式文件的版本号和表示终端101与接入点102间的通信速度的信息传达给文件服务器103，基于文件服务器103取得的信息，决定版本修改的有无和更新处理方针，向终端101回答决定的内容。

此外，在第二至第四实施例中，是终端101调查通信速度，但也可以由接入点102调查通信速度传达给终端101。

另外，在第二至第四实施例中，根据终端101与接入点102间的通信速度决定更新处理方针，但不限于此，也可以根据终端101与例如文件服务器103间的通信速度决定更新方针。该情况下，调查通信速度的设备无论是终端101还是文件服务器103都行。

此外，在第一至第四实施例中，都说明了反病毒程序的模式文件更新处理的情况。但是，本发明不限于此，也可以应用于适用终端101工作的反病毒程序自身的版本修改，和修正OS及应用程序软件中的不当之处的补丁时的这些内容的下载。

此外，在第二至第四实施例中，都着眼于通信速度（通信频带）决定更新处理方针，但也可以在决定更新处理方针时，在通信速度之外也考虑终端101的连接处。

例如，考虑终端101是具有无线LAN终端和携带式电话机双重功能的情况。在终端101与携带电话网连接的情况下，通信频带窄而且花费信息包通信等的通信成本，所以就抑制下载，另一方面，在能与通信频带宽且成本便宜的无线LAN连接的情况下，就实行下载。

这样，在削减了通信成本的基础上，不损伤模式文件更新时的用户的舒适性，而且能进行高度的安全措施。

此外，例如，若考虑到从游园地等文化娱乐中心接受在园内进行的加演节目和用无线发送到终端的电影和音乐等内容的连接服务的情况，为了抑制加演节目和内容的发送的同步的偏移，可以考虑抑制模式文件的下载为好。作为具体的抑制方法，有例如设定用于判断模式文件的下载的阈值（通信频带、模式文件的重要性的评价标准等）为高值的方法，和强制利用屏蔽服务器的方法等。

其它优点和变型对于本领域的技术人员来说可以很容易地想到。因此，广义而言，本发明并不限于上面的详细描述和有代表性的实施方式。所以，在不脱

离如所附权利要求所限定的本发明的精神和范围的前提下可作出各种变型。

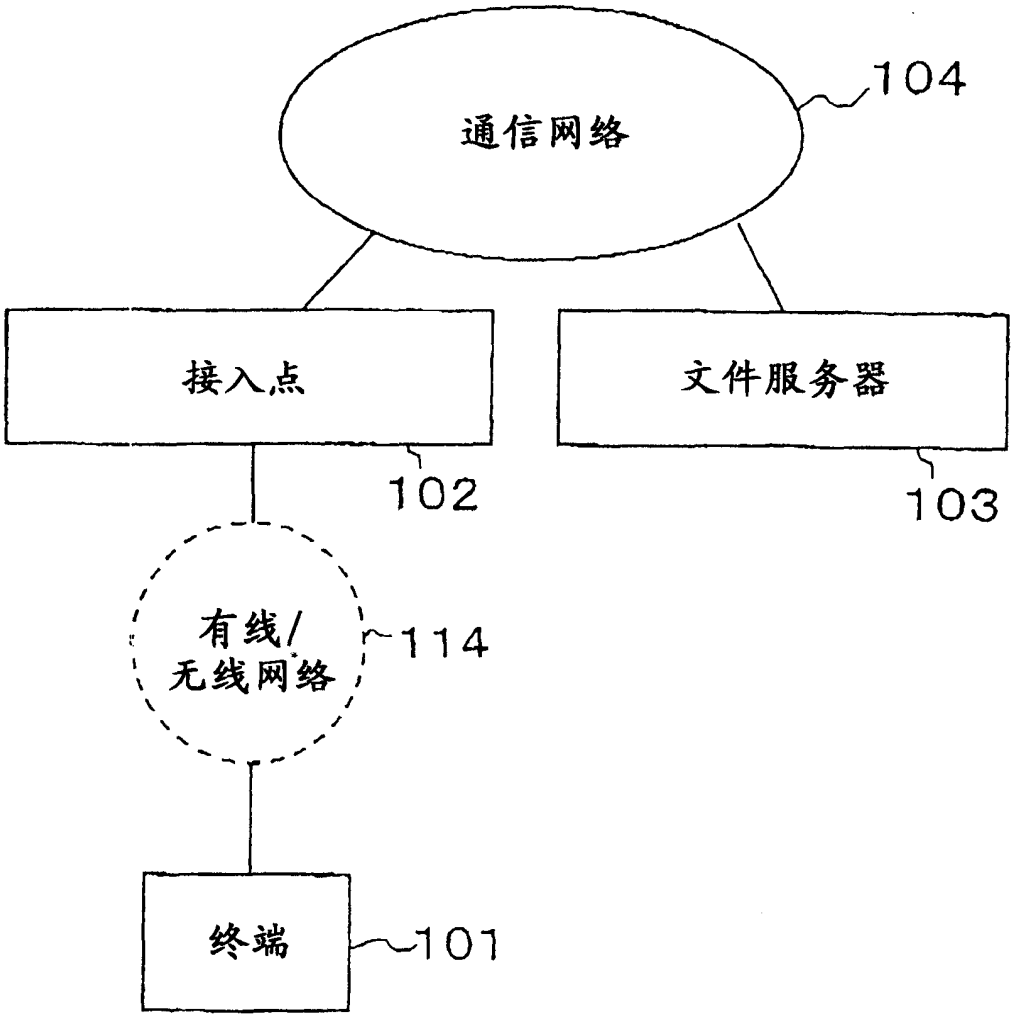


图1

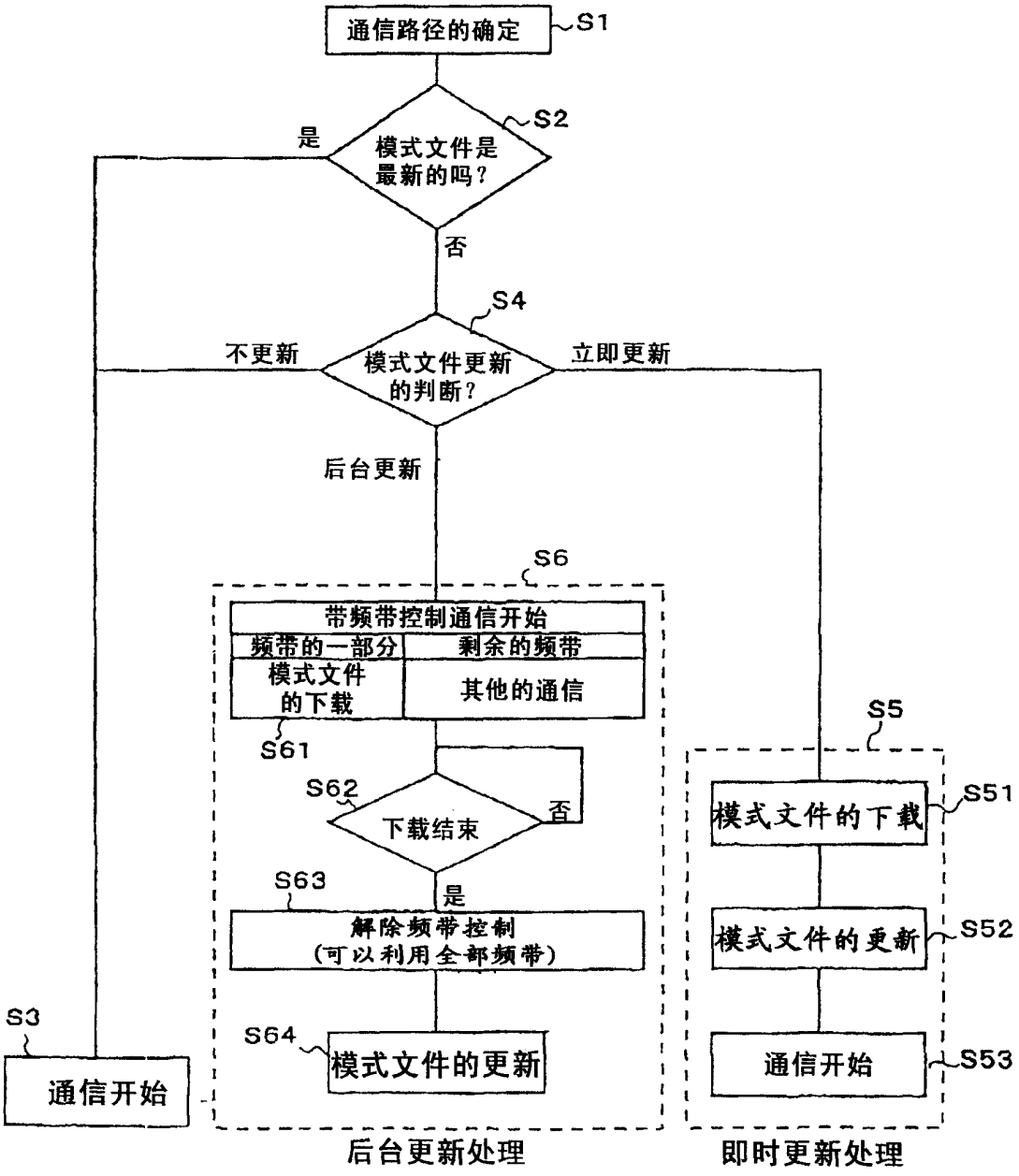

通信路径的确定
S1
S2
是
模式文件是最新的吗？
否
S4
不更新
模式文件更新的判断？
立即更新
后台更新
S6
带频带控制通信开始
频带的一部分
剩余的频带
模式文件的下载
其他的通信
S61
S62
下载结束
否
S63
是
解除频带控制（可以利用全部频带）
S64
模式文件的更新
S3
通信开始
后台更新处理
S5
模式文件的下载
S51
模式文件的更新
S52
通信开始
S53
即时更新处理

图2

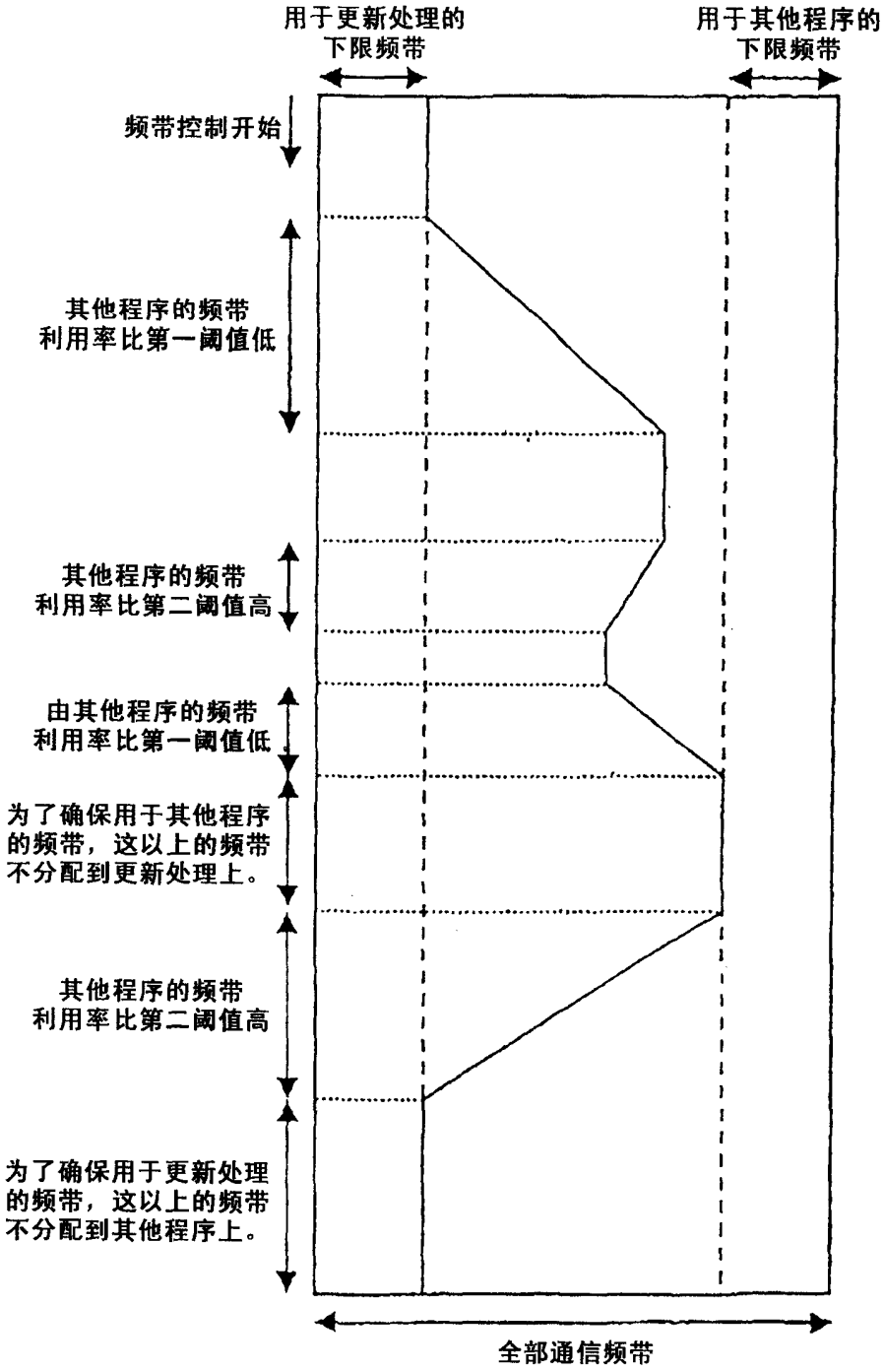

用于更新处理的
下限频带
用于其他程序的
下限频带
频带控制开始
其他程序的频带
利用率比第一阈值低
其他程序的频带
利用率比第二阈值高
由其他程序的频带
利用率比第一阈值低
为了确保用于其他程序
的频带，这以上的频带
不分配到更新处理上。
其他程序的频带
利用率比第二阈值高
为了确保用于更新处理
的频带，这以上的频带
不分配到其他程序上。
全部通信频带

图3

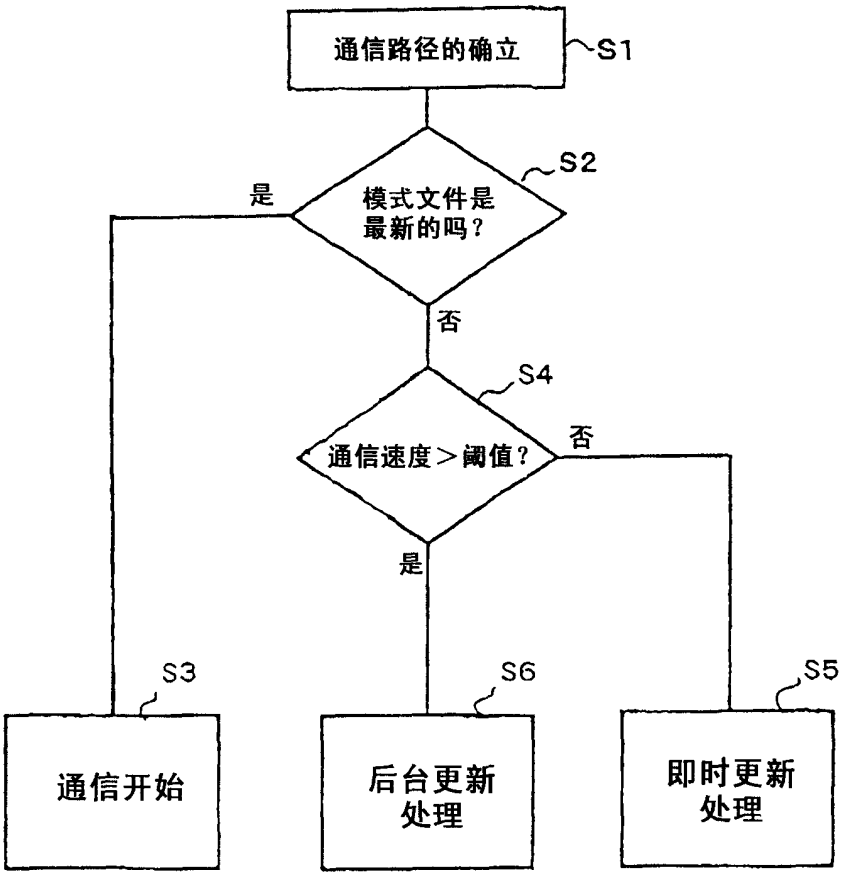

通信路径的确立
S1
S2
模式文件是
最新的吗？
是
否
S4
通信速度＞阈值？
否
是
S3
S6
S5
通信开始
后台更新
处理
即时更新
处理

图 4

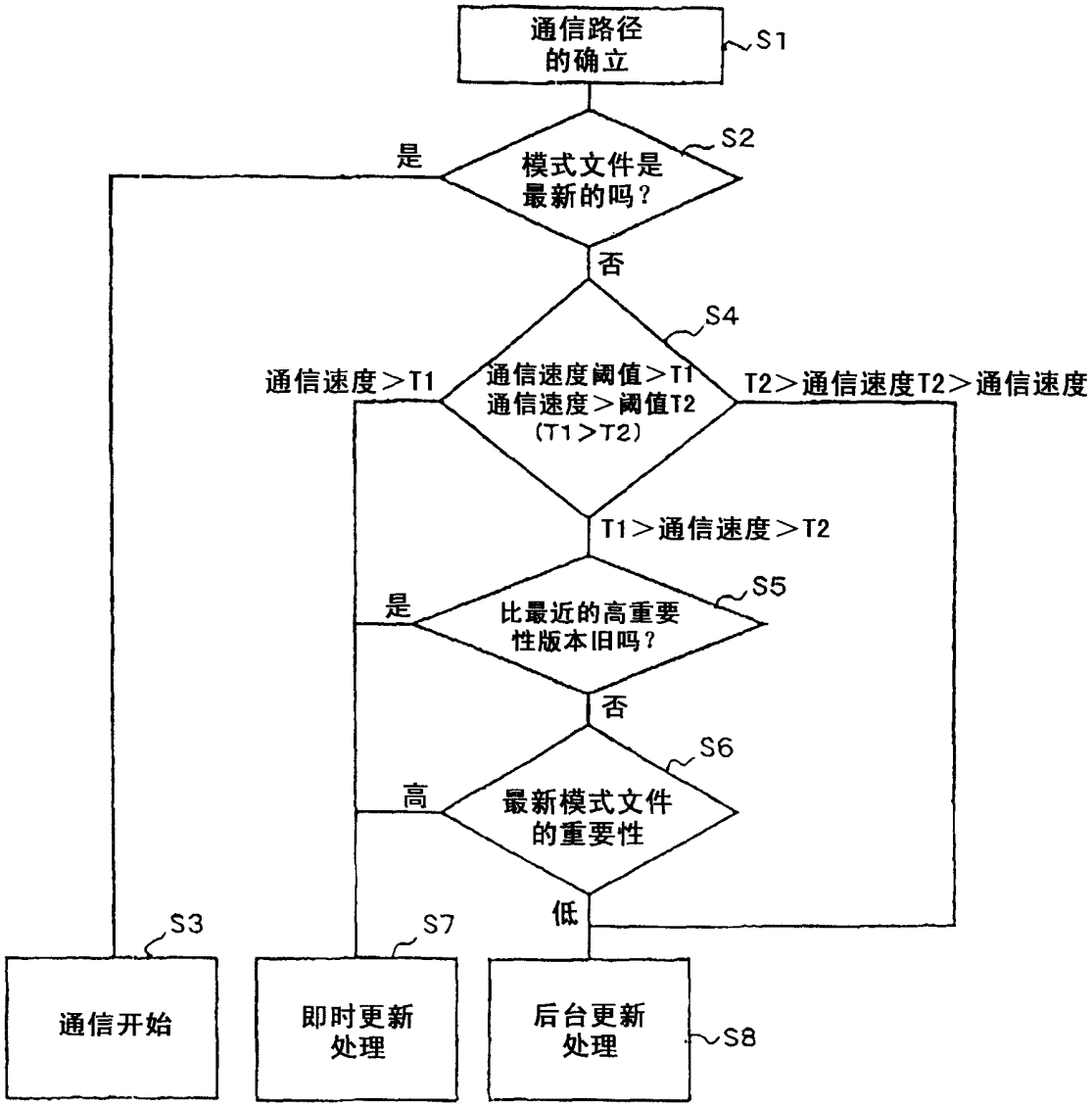

通信路径
的确立
S1
S2
是
模式文件是
最新的吗？
否
S4
通信速度＞T1
通信速度阈值＞T1
通信速度＞阈值T2
(T1＞T2)
T2＞通信速度T2＞通信速度
T1＞通信速度＞T2
S5
是
比最近的高重要
性版本旧吗？
否
S6
高
最新模式文件
的重要性
低
S3
S7
通信开始
即时更新
处理
后台更新
处理
S8

图5

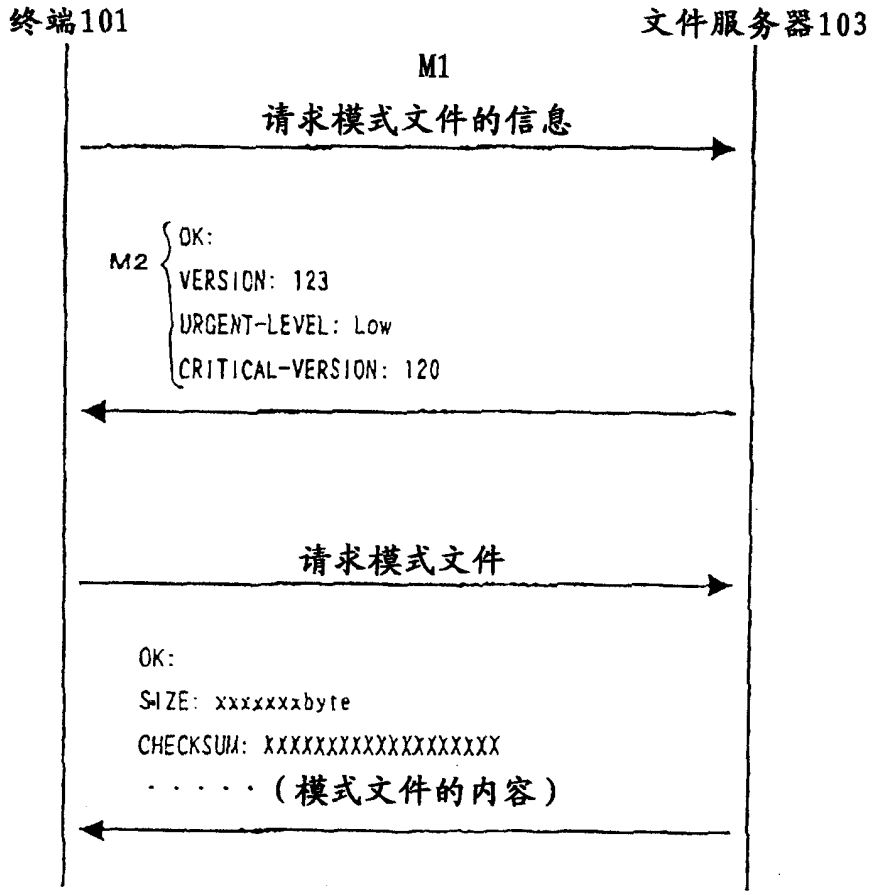

终端101
文件服务器103
M1
请求模式文件的信息
M2
OK:
VERSION: 123
URGENT-LEVEL: Low
CRITICAL-VERSION: 120
请求模式文件
OK:
SIZE: xxxxxxxbyte
CHECKSUM: XXXXXXXXXXXXXXXXX
·····（模式文件的内容）

图6

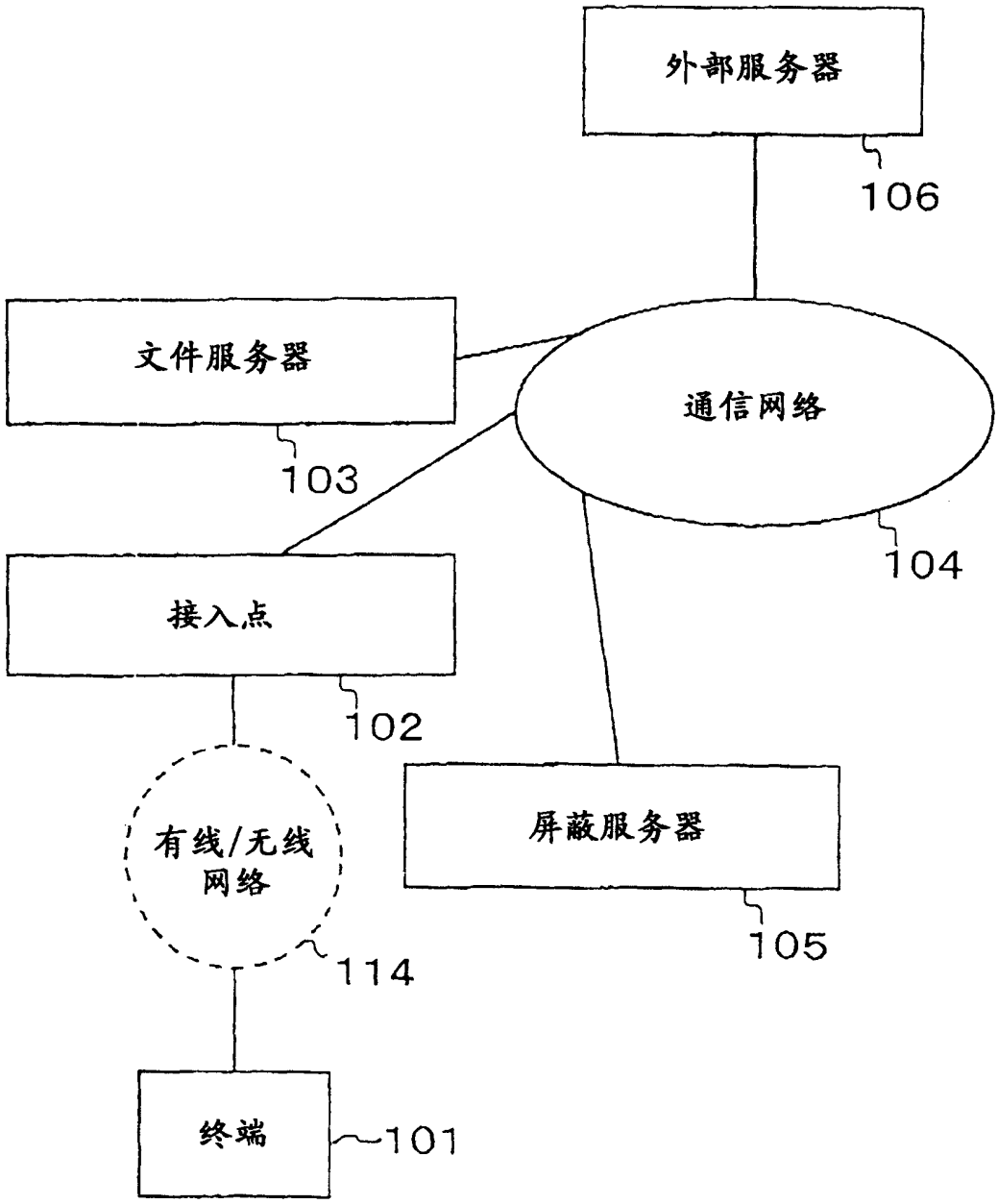

外部服务器
106
文件服务器
103
通信网络
104
接入点
102
有线/无线
网络
114
屏蔽服务器
105
终端
101

图7

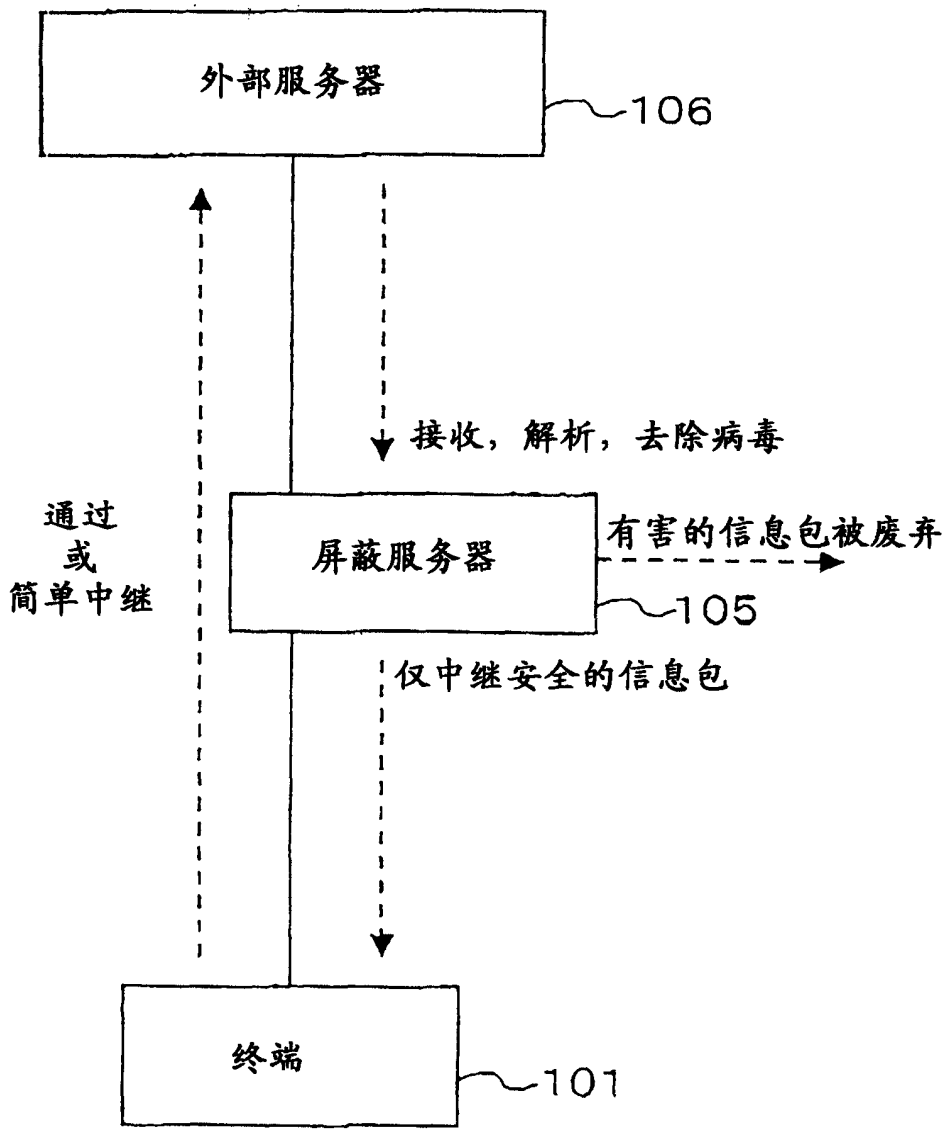

外部服务器
106
接收，解析，去除病毒
通过
或
简单中继
屏蔽服务器
有害的信息包被废弃
105
仅中继安全的信息包
终端
101

图8

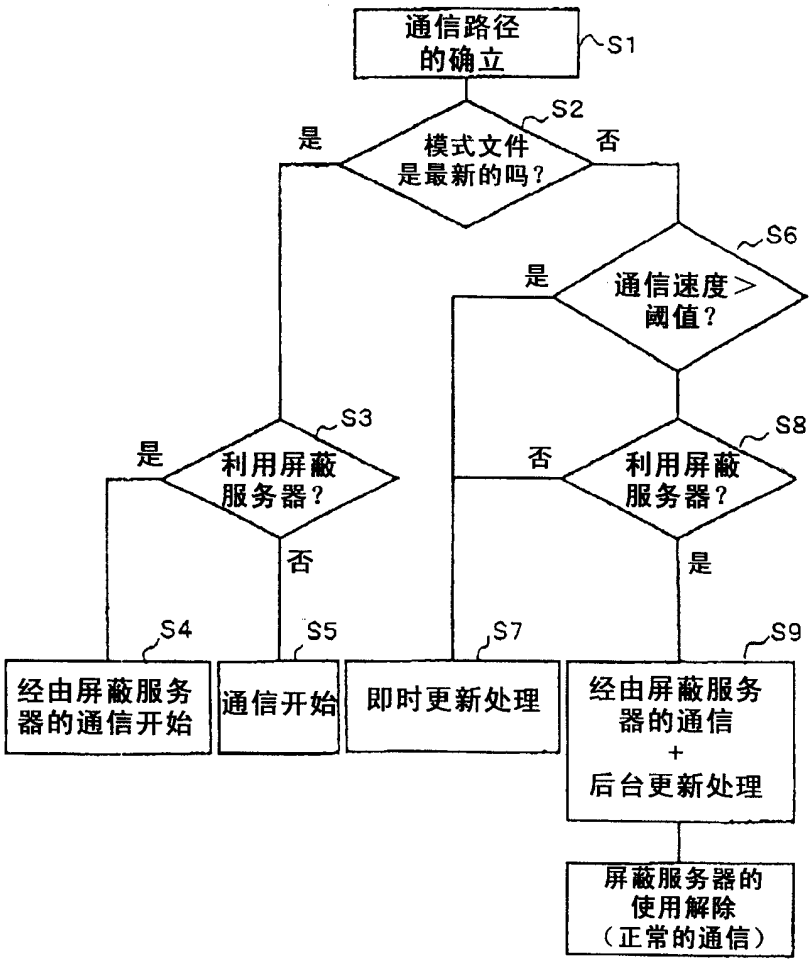

通信路径
的确立
S1
S2
模式文件
是最新的吗？
是
否
S6
通信速度＞
阈值？
是
S3
利用屏蔽
服务器？
是
否
S8
利用屏蔽
服务器？
否
是
S4
S5
S7
S9
经由屏蔽服务
器的通信开始
通信开始
即时更新处理
经由屏蔽服务
器的通信
+
后台更新处理
屏蔽服务器的
使用解除
（正常的通信）

图9