

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06F 1/00 (2006.01)  
H04L 29/06 (2006.01)



# [12] 发明专利申请公布说明书

[21] 申请号 200580041061.1

[43] 公开日 2007年11月7日

[11] 公开号 CN 101069145A

[22] 申请日 2005.8.10

[21] 申请号 200580041061.1

[30] 优先权

[32] 2004.9.30 [33] US [31] 10/711,730

[32] 2004.10.1 [33] US [31] 10/956,832

[32] 2004.10.1 [33] US [31] 10/956,764

[86] 国际申请 PCT/US2005/028607 2005.8.10

[87] 国际公布 WO2006/038987 英 2006.4.13

[85] 进入国家阶段日期 2007.5.30

[71] 申请人 茨特里克斯系统公司

地址 美国佛罗里达州

[72] 发明人 R·G·布拉迪 T·西蒙斯

A·D·库克里尔 P·N·卡尔文

[74] 专利代理机构 中国专利代理(香港)有限公司  
代理人 王岳 陈景峻

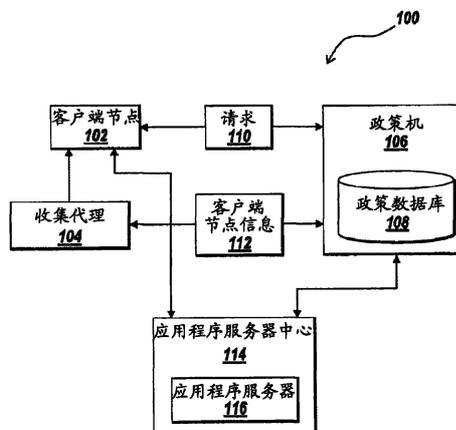
权利要求书 11 页 说明书 26 页 附图 11 页

## [54] 发明名称

在提供访问联网内容文件中分配访问控制级的方法和设备

## [57] 摘要

公开了当提供访问联网内容文件时,用于分配访问控制级的方法和设备,该设备包括客户端节点(102)、收集代理(104)、以及政策机(106)。客户端节点请求访问资源。收集代理收集关于该客户端节点的信息。政策机接收所收集的信息并且响应于政策的应用程序分配多个访问级之一给所接收的信息。应用程序服务器中心(114)可以使用与所请求的文件的文件类型有关的应用程序将资源内容呈现给客户端节点。转换服务器(516)可以将资源内容从原始格式转换为第二格式并且将所转换的资源内容呈现给客户端节点。



1. 一种准许访问资源的系统，包括：
  - a. 客户端节点，其请求访问资源；
  - b. 收集代理，其收集关于该客户端节点的信息；以及
  - c. 政策机，其接收所收集的信息并且响应于政策的应用程序分配多个访问级之一给所接收的信息。
2. 根据权利要求 1 的系统，其中所述政策机进一步包括存储可配置政策的数据库。
3. 根据权利要求 1 的系统，其中系统管理员在政策机中配置政策以提供访问控制权级给客户端节点。
4. 根据权利要求 1 的系统，其中所述政策机传送指令给收集代理确定收集代理所收集的信息的类型。
5. 根据权利要求 1 的系统，其中所述政策机进一步包括登录上网代理。
6. 根据权利要求 5 的登录上网代理，其中所述登录上网代理从收集代理接收所收集的信息。
7. 根据权利要求 5 的登录上网代理，其中所述登录上网代理为所述政策机识别出从所述收集代理接收的认证信息。
8. 根据权利要求 1 的系统，其中所述政策机进一步包括多个登录上网代理。
9. 根据权利要求 8 的系统，其中所述多个登录上网代理的至少一个位于每个网络域，客户端节点可以从所述每个网络域传送资源请求。
10. 根据权利要求 9 的系统，其中所述客户端节点传送所述资源请求给特定的登录上网代理。
11. 根据权利要求 10 的系统，其中所述登录上网代理为政策机识别出所述网络域，客户端节点可以从所述网络域传送资源请求。
12. 根据权利要求 1 的系统，其中所述收集代理在客户端节点上执行。
13. 根据权利要求 1 的系统，其中所述政策机传送收集代理给客户端节点。
14. 根据权利要求 1 的系统，其中所述收集代理包括至少一个脚

本。

15. 根据权利要求 1 的系统，其中所述收集代理包括字节码。

16. 根据权利要求 1 的系统，其中所述收集代理通过在客户端节点上运行至少一个脚本来收集信息。

17. 根据权利要求 1 的系统，其中所述收集代理收集关于客户端节点的信息，所述信息位于服务器上。

18. 根据权利要求 17 的系统，其中所述收集代理收集包括 HTTP 报头的信息。

19. 根据权利要求 17 的系统，其中所述收集代理收集包括客户端节点的网络区域的信息。

20. 根据权利要求 17 的系统，其中所述收集代理收集包括由客户端节点使用的认证方法的信息。

21. 根据权利要求 1 的系统，其中所述收集代理收集客户端节点的机器 ID。

22. 根据权利要求 1 的系统，其中所述收集代理收集包括操作系统类型的信息。

23. 根据权利要求 1 的系统，其中所述收集代理收集包括操作系统补丁的存在的信息。

24. 根据权利要求 1 的系统，其中所述收集代理收集包括安装的网络卡的 MAC 地址的信息。

25. 根据权利要求 1 的系统，其中所述收集代理收集包括客户端设备上的水印的信息。

26. 根据权利要求 1 的系统，其中所述收集代理收集包括有效目录中的从属关系的信息。

27. 根据权利要求 1 的系统，其中所述收集代理收集包括病毒扫描软件的存在的信息。

28. 根据权利要求 1 的系统，其中所述收集代理收集包括防火墙的存在的信息。

29. 根据权利要求 1 的系统，其中所述收集代理收集包括 HTTP 报头的信息。

30. 一种准许访问资源的方法，该方法包括：

a. 客户端节点请求访问资源；

- b. 收集代理收集关于该客户端节点的信息;
- c. 政策机接收所收集的信息;
- d. 以及
- e. 基于所接收的信息做出访问控制决定。

31. 根据权利要求 30 的方法, 其中步骤 (a) 进一步包括通过网络连接请求资源。

32. 根据权利要求 30 的方法, 其中步骤 (b) 进一步包括通过网络连接收集信息。

33. 根据权利要求 30 的方法, 其中步骤 (b) 进一步包括通过在客户端节点上执行至少一个脚本来收集信息。

34. 根据权利要求 30 的方法, 其中步骤 (c) 进一步包括判定所接收的信息是否满足条件。

35. 根据权利要求 34 的方法, 进一步包括通过比较所接收的信息与至少一个条件来判定所接收的信息是否满足条件。

36. 根据权利要求 35 的方法, 其中步骤 (d) 进一步包括通过应用政策到所述条件做出访问控制决定。

37. 一种政策机, 包括:

a. 第一部件, 其接收关于客户端节点的信息, 并且从该信息生成数据组;

b. 第二部件, 其接收该数据组, 并且基于该数据组将可用于该客户端的资源的枚举提供给第一部件。

38. 根据权利要求 37 的政策机, 其中所述第一部件从收集代理接收信息。

39. 根据权利要求 37 的政策机, 其中所述第一部件包括所接收的信息与之比较的至少一个条件。

40. 根据权利要求 37 的政策机, 其中所述第二部件进一步包括数据库。

41. 根据权利要求 40 的政策机, 其中所述数据库存储至少一个政策。

42. 根据权利要求 41 的政策机, 其中所述第二部件进一步包括通过应用所述至少一个政策到所述数据组来识别可用资源。

43. 根据权利要求 37 的政策机, 其中所述政策机进一步包括登

录上网代理。

44. 根据权利要求 43 的登录上网代理，其中所述登录上网代理从收集代理接收所收集的信息。

45. 根据权利要求 44 的登录上网代理，其中所述登录上网代理为所述政策机识别出从所述收集代理接收的认证信息。

46. 根据权利要求 43 的政策机，其中所述政策机进一步包括多个登录上网代理。

47. 根据权利要求 46 的系统，其中所述多个登录上网代理的至少一个位于每个网络域上，客户端节点可以从每个网络域传送资源请求。

48. 根据权利要求 47 的政策机，其中所述客户端节点传送资源请求给特定登录上网代理。

49. 一种使用政策机准许访问的方法，该方法包括：

- a. 第一部件接收关于客户端节点的信息；
- b. 第一部件从该信息生成数据组；
- c. 以及
- d. 第二部件提供可用于所述客户端的资源的枚举。

50. 根据权利要求 49 的方法，进一步包括第二部件基于所述数据组识别可用于所述客户端节点的资源的步骤。

51. 根据权利要求 50 的方法，进一步包括通过应用政策到所接收的数据组来识别出可用资源。

52. 根据权利要求 49 的方法，进一步包括请求的步骤。

53. 根据权利要求 49 的方法，进一步包括接收关于客户端节点的另外信息的步骤。

54. 根据权利要求 49 的方法，其中步骤 (c) 进一步包括第二部件应用政策到所接收的信息以决定可用于所述客户端节点的访问方法。

55. 根据权利要求 49 的方法，其中步骤 (c) 进一步包括第一部件接收所述可用资源的枚举。

56. 根据权利要求 55 的方法，其中步骤 (c) 进一步包括第一部件接收可用资源的子集的枚举。

57. 根据权利要求 55 的方法，其中步骤 (c) 进一步包括第一部

件提供所述枚举给所述客户端节点。

58. 根据权利要求 55 的方法, 其中步骤 (c) 进一步包括第一部件在 HTML 网页上提供所述枚举给客户端节点。

59. 一种提供文件内容的方法, 包括步骤:

- a. 客户端节点传送文件请求;
- b. 访问控制服务器接收文件请求;
- c. 访问控制服务器做出访问控制决定;
- d. 确定该文件的文件类型;
- e. 确定与文件类型有关的应用程序的标识符; 以及
- f. 将文件内容呈现给所述客户端节点。

60. 根据权利要求 59 的方法, 其中步骤 (f) 进一步包括应用程序服务器中心中的应用程序服务器将文件内容呈现给所述客户端节点。

61. 根据权利要求 59 的方法, 进一步包括应用程序服务器中心中的第一应用程序服务器确定与所述文件类型有关的应用程序。

62. 根据权利要求 61 的方法, 进一步包括应用程序服务器中心中的第一应用程序服务器将文件内容呈现给所述客户端节点。

63. 根据权利要求 61 的方法, 进一步包括应用程序服务器中心中的第二应用程序服务器将文件内容呈现给所述客户端节点。

64. 根据权利要求 59 的方法, 其中步骤 (d) 进一步包括访问控制服务器确定所述文件的文件类型。

65. 根据权利要求 59 的方法, 其中步骤 (d) 进一步包括应用程序服务器中心中的应用程序服务器确定所述文件的文件类型。

66. 根据权利要求 59 的方法, 其中步骤 (e) 进一步包括访问控制服务器确定与所述文件类型有关的应用程序的标识符。

67. 根据权利要求 59 的方法, 其中步骤 (e) 进一步包括应用程序服务器中心中的应用程序服务器确定与所述文件类型有关的应用程序的标识符。

68. 根据权利要求 59 的方法, 进一步包括访问控制服务器获取关于所述客户端节点的信息。

69. 根据权利要求 68 的方法, 其中步骤 (c) 进一步包括比较由所述访问控制服务器获取的信息与政策以做出所述访问控制决定。

70. 根据权利要求 68 的方法, 其中步骤 (f) 进一步包括应用程序服务器使用所获取的信息来选择用于呈现文件内容的格式。

71. 根据权利要求 68 的方法, 其中步骤 (f) 进一步包括通过将政策应用到所获取的信息来呈现文件内容以选择用于呈现所述文件内容的格式。

72. 根据权利要求 59 的方法, 进一步包括访问控制服务器传送收集代理给所述客户端节点的步骤。

73. 根据权利要求 59 的方法, 进一步包括访问控制服务器使用收集代理获取关于所述客户端节点的信息。

74. 根据权利要求 73 的方法, 其中步骤 (c) 进一步包括比较由所述收集代理获取的信息与政策以做出访问控制决定。

75. 根据权利要求 59 的方法, 其中步骤 (c) 进一步包括访问控制服务器拒绝所述请求。

76. 根据权利要求 59 的方法, 其中步骤 (d) 进一步包括访问控制服务器通过提取文件扩展名判定所述文件类型。

77. 根据权利要求 59 的方法, 其中步骤 (e) 进一步包括应用程序服务器通过使用文件扩展名查询用于该应用程序的数据库来判定应用程序的标识符。

78. 根据权利要求 59 的方法, 进一步包括从文件服务器取回所述文件的步骤。

79. 根据权利要求 78 的方法, 进一步包括应用程序服务器从文件服务器取回所述文件的步骤。

80. 根据权利要求 78 的方法, 进一步包括访问控制服务器从文件服务器取回所述文件的步骤。

81. 根据权利要求 59 的方法, 进一步包括从 web 服务器取回所述文件的步骤。

82. 根据权利要求 81 的方法, 进一步包括应用程序服务器从 web 服务器取回所述文件的步骤。

83. 根据权利要求 81 的方法, 进一步包括访问控制服务器从 web 服务器取回所述文件的步骤。

84. 根据权利要求 59 的方法, 进一步包括从电子邮件服务器取回所述文件的步骤。

85. 根据权利要求 84 的方法, 进一步包括应用程序服务器从电子邮件服务器取回所述文件的步骤。

86. 根据权利要求 84 的方法, 进一步包括访问控制服务器从电子邮件服务器取回所述文件的步骤。

87. 根据权利要求 59 的方法, 进一步包括所述客户端节点连接到应用程序服务器的步骤。

88. 根据权利要求 87 的方法, 其中步骤 (f) 进一步包括通过所述连接将所述文件内容呈现给所述客户端节点。

89. 根据权利要求 59 的方法, 进一步包括访问控制服务器传送可执行文件给所述客户端节点的步骤。

90. 根据权利要求 89 的方法, 进一步包括可执行文件识别打开所述客户端节点的文件的应用程序服务器。

91. 根据权利要求 59 的方法, 其中步骤 (a) 进一步包括所述客户端节点位于通过网络边界与第二网络分隔开的第一网络上, 所述客户端节点从位于所述第二网络上的访问控制服务器请求文件。

92. 根据权利要求 85 的方法, 其中步骤 (d) 进一步包括访问控制服务器从内容服务器下载所述文件。

93. 一种用于提供文件内容的系统, 包括:

a. 请求文件的客户端节点;

b. 访问控制服务器, 其接收用于所述文件的请求并且做出访问控制决定;

以及

c. 应用程序服务器, 其使用与所请求的文件的文件类型有关的应用程序将所述文件内容呈现给所述客户端节点。

94. 根据权利要求 93 的系统, 其中所述应用程序服务器进一步包括识别与所述文件类型有关的应用程序。

95. 根据权利要求 93 的系统, 其中所述访问控制服务器进一步包括识别与所述文件类型有关的应用程序。

96. 根据权利要求 93 的系统, 其中所述访问控制服务器进一步包括存储至少一个政策的数据库。

97. 根据权利要求 93 的系统, 其中所述访问控制服务器进一步包括获取关于客户端节点的信息的收集代理。

98. 根据权利要求 97 的系统, 其中所述访问控制服务器进一步包括基于由所述收集代理获取的信息做出访问控制决定。

99. 根据权利要求 97 的系统, 其中所述访问控制服务器进一步包括通过应用政策到由所述收集代理获取的信息做出访问控制决定。

100. 根据权利要求 97 的系统, 其中所述收集代理获取关于客户端节点的有关设备类型的信息。

101. 根据权利要求 97 的系统, 其中所述收集代理获取关于客户端节点的有关网络连接信息的信息。

102. 根据权利要求 97 的系统, 其中所述收集代理获取关于客户端节点的有关授权证书的信息。

103. 根据权利要求 93 的系统, 其中所述应用程序服务器包括数据库, 该数据库包含与至少一个文件类型有关的至少一个应用程序。

104. 根据权利要求 103 的系统, 其中所述应用程序服务器进一步包括通过查询所述数据库判定应用程序的标识符。

105. 根据权利要求 93 的系统, 其中所述访问控制服务器传送可执行文件给所述客户端节点。

106. 根据权利要求 105 的系统, 其中所述可执行文件包括与所述文件有关的所述应用程序的标识符。

107. 根据权利要求 105 的系统, 其中所述可执行文件识别应用程序服务器。

108. 根据权利要求 105 的系统, 其中所述客户端节点进行到由所述可执行文件识别的应用程序服务器的连接。

109. 根据权利要求 105 的系统, 其中所述应用程序服务器接受来自所述客户端节点的连接。

110. 根据权利要求 105 的系统, 其中所述客户端节点传送由所述可执行文件识别的所述应用程序的标识符到所述应用程序服务器。

111. 根据权利要求 105 的系统, 其中所述应用程序服务器通过所述连接将文件内容呈现给所述客户端节点。

112. 一种准许访问资源的系统, 包括:

- a. 客户端节点, 其请求访问资源;
- b. 收集代理, 其收集关于客户端节点的信息;
- c. 政策机, 其接收所收集的信息并且基于所接收的信息做出访

问控制决定；以及

d. 转换服务器，其从政策机接收文件请求，将文件内容从原始格式转换成第二格式，并且将所转换的文件内容呈现给客户端节点。

113. 根据权利要求 112 的系统，其中所述转换服务器通过代理服务器接收来自所述政策机的文件请求。

114. 根据权利要求 112 的系统，其中所述政策机基于应用政策到所收集的信息做出访问控制决定。

115. 根据权利要求 112 的系统，其中所述政策机进一步包括数据库。

116. 根据权利要求 112 的系统，其中所述政策机进一步包括登录上网代理。

117. 根据权利要求 116 的登录上网代理，其中所述登录上网代理从所述收集代理接收所收集的信息。

118. 根据权利要求 112 的系统，其中所述收集代理在所述客户端节点上执行。

119. 根据权利要求 112 的系统，其中所述政策机传送所述收集代理给所述客户端节点。

120. 根据权利要求 112 的系统，其中所述收集代理包括至少一个脚本。

121. 根据权利要求 112 的系统，其中所述收集代理包括字节码。

122. 根据权利要求 112 的系统，其中所述政策机传送指令到所述收集代理来确定收集代理收集的信息的类型。

123. 根据权利要求 112 的系统，其中所述收集代理通过在所述客户端节点上运行至少一个脚本来收集信息。

124. 根据权利要求 112 的系统，其中所述收集代理收集有关所述客户端节点设备类型的信息。

125. 根据权利要求 112 的系统，其中所述收集代理收集有关所述客户端节点网络连接的信息。

126. 根据权利要求 112 的系统，其中所述收集代理收集包括浏览器类型的信息。

127. 根据权利要求 112 的系统，其中所述收集代理收集包括操作系统类型的信息。

128. 一种准许访问资源的方法，该方法包括：

- a. 客户端节点请求访问文件；
- b. 收集代理收集关于客户端节点的信息；
- c. 政策机接收所收集的信息；
- d. 基于所接收的信息做出访问控制决定；
- e. 转换服务器将文件内容从原始格式转换成第二格式；并且
- f. 转换服务器将所转换的文件内容呈现给客户端节点。

129. 根据权利要求 128 的方法，进一步包括政策机传送所述文件请求给转换服务器。

130. 根据权利要求 128 的方法，进一步包括通过代理服务器路由所述文件请求给所述转换服务器。

131. 根据权利要求 128 的方法，进一步包括政策机通过代理服务器路由所述文件请求给所述转换服务器。

132. 根据权利要求 128 的方法，其中步骤 (a) 进一步包括通过网络连接请求所述资源。

133. 根据权利要求 128 的方法，其中步骤 (b) 进一步包括所述收集代理通过网络连接收集所述信息。

134. 根据权利要求 128 的方法，其中步骤 (b) 进一步包括所述收集代理通过在所述客户端节点上执行至少一个脚本收集所述信息。

135. 根据权利要求 128 的方法，其中步骤 (c) 进一步包括所述政策机判定所接收的信息是否满足条件。

136. 根据权利要求 128 的方法，进一步包括政策机通过比较所接收的信息与至少一个条件来判定所接收的信息是否满足条件。

137. 根据权利要求 136 的方法，其中步骤 (d) 进一步包括政策机通过应用政策到所述条件来做出访问控制决定。

138. 一种政策机，包括：

a. 第一部件，其接收关于客户端节点的信息，并且从所接收的信息生成数据组；以及

b. 第二部件，其接收所述数据组，并且基于所述数据组将可用于所述客户端的资源的枚举提供给所述第一部件。

139. 根据权利要求 138 的政策机，其中所述第一部件从收集代理接收信息。

140. 根据权利要求 138 的政策机，其中所述第一部件包括所接收的信息与之比较的至少一个条件。

141. 根据权利要求 138 的政策机，其中所述第二部件进一步包括数据库。

142. 根据权利要求 141 的政策机，其中所述数据库存储至少一个政策。

143. 根据权利要求 142 的政策机，其中所述第二部件进一步包括通过应用所述至少一个政策到所述数据组来识别可用资源。

144. 一种准许使用政策机访问的方法，该方法包括：

- a. 第一部件接收关于客户端节点的信息；
- b. 第一部件从所述信息生成数据组；以及
- c. 第二部件提供可用于所述客户端的资源的枚举。

145. 根据权利要求 144 的方法，进一步包括第二部件基于所述数据组识别可用于所述客户端节点的资源的步骤。

146. 根据权利要求 145 的方法，进一步包括通过应用政策到所接收的数据组识别可用资源。

147. 根据权利要求 144 的方法，进一步包括请求关于所述客户端节点的信息的步骤。

148. 根据权利要求 144 的方法，进一步包括接收关于所述客户端节点的另外信息的步骤。

149. 根据权利要求 144 的方法，其中步骤 (b) 进一步包括第一部件应用政策到所接收的信息来确定可用于所述客户端节点的访问方法。

150. 根据权利要求 144 的方法，其中步骤 (c) 进一步包括第二部件提供可用资源的子组的枚举给所述客户端节点。

151. 根据权利要求 144 的方法，其中步骤 (c) 进一步包括第一部件接收可用资源的枚举。

152. 根据权利要求 151 的方法，其中步骤 (c) 进一步包括第一部件提供所述枚举给所述客户端节点。

153. 根据权利要求 151 的方法，其中步骤 (c) 进一步包括第一部件在 HTML 网页上提供所述枚举给所述客户端节点。

## 在提供访问联网内容文件中分配访问控制级的方法和设备

### 技术领域

本发明涉及用于安全访问联网资源的方法和设备，并且具体地，涉及用于在从服务器提供访问联网内容文件中分配访问控制级的方法和设备。

### 背景技术

按照惯例，客户端系统上的用户使用 web 浏览器和其它基于客户端的应用程序来访问从远端位置取回的内容文件。例如，用户可以使用华盛顿州的雷蒙德 (Redmond) 的微软公司的 INTERNET EXPLORER 访问互联网内容，并且然后使用也来自微软公司的 WINDOWS EXPLORER 来访问桌面产品文件类型，比如已经被下载到本地位置的 WORD 文档。

常规的处理要求下载文件到客户端节点用于观看和处理。然而，从安全性观点看，这种处理存在问题。为了访问客户端上的内容，要求用户两次本地保存该内容到非易失存储器。在下载期间要求第一次保存，并且在上传处理之前编辑之后要求第二次保存。而且，许多用户经常从一个本地目录移动和/或拷贝下载的内容到另一个本地目录 (例如，从 dir://downloaded-files 到 dir://my-documents)。这些保存动作的每一个在客户端创建了该文档的一个本地拷贝。客户端设备的极少用户将记得手动删除所述文档的这些本地拷贝，这些拷贝因此保留在客户端设备上。

此外，客户端设备的存储器的直接处理对用户来说可能难接近的，比如其中客户端设备位于公用电话亭环境中的情况。在这些情况中，删除本地拷贝的选项对用户来说并不是可以做到的。因为留在客户端上的文档可能是由未被授权的个人通过访问客户端机器所访问的，这提出了显著的安全性问题。另外，较小的设备类型，比如个人数字助理，可能没有足够的资源来允许在设备上使用基于客户端的应用程序。

为了试图解决这些顾虑，常规的访问控制方法在准许访问之前可能要求来自客户端的特定认证证书 (authentication credential) 并

且可能拒绝来自不合法位置或设备的访问。然而，常规方法的局限性是通常要求访问控制决定引起要么拒绝要么准许访问资源。在拒绝的情况下，该方法不能提供任何可替换的访问方法。在准许的情况下，该方法可以提供仅完全的和完整的资源公开。通过基于访问控制级分配访问等级来准许访问控制的方法在联网环境中提供对私有资源（proprietary resource）的访问时是所希望的。

另外，在保护私有数据不受到不合法客户端节点的访问中，访问权根据诸如客户端设备类型、授权（authorization）证书、以及性能之类的因素来提供访问文件的可替换方法是所希望的。完全拒绝访问权的一种替换方案（比如代表客户端对在安全网络上执行的文件的有限权利）是所希望的。

### 发明内容

本发明涉及通过分配多个访问级之一用于安全访问来自服务器的内容文件以实现增强安全性、证据收集、以及政策应用程序从而提供访问控制的方法和设备。

在一个方面中，本发明涉及用于准许访问资源的系统和方法。客户端节点请求访问资源。收集代理收集关于该客户端节点的信息并且政策机接收所收集的信息。政策机通过响应于政策的应用程序分配多个访问级之一给所接收的信息来做出访问控制决定。

在一个实施例中，政策机通过应用政策到所接收的信息做出访问决定。在另一个实施例中，政策机传送该收集代理给客户端节点。

在另一个方面中，本发明涉及用于准许访问资源的方法和设备。该设备包括政策机，该政策机包括两个部件。第一部件接收关于客户端节点的信息并且从该信息生成数据组。第二部件接收该数据组，并且基于所接收的数据组将可用于该客户端的资源的枚举（enumeration）提供给第一部件。第一部件将所述资源的枚举呈现给客户端节点。

在一个实施例中，第一部件从收集代理接收信息。在一个实施例中，每个部件另外包括数据库。第一部件中的数据库存储条件。第二部件中的数据库存储政策。第一部件应用条件到所接收的信息并且第二部件应用政策到所接收的数据组。在另一个实施例中，第二部件生

成可用于客户端节点的资源子组的枚举。

本发明还涉及用于访问网络资源以实现增强的安全性从而减少联网环境中的私有数据的公开的方法和设备。

在一个方面中，本发明涉及用于提供文件内容的方法和设备。客户端节点传送文件请求。访问控制服务器接收该请求并且做出访问控制决定。应用程序服务器中心(application server farm)使用与所请求文件的文件类型有关的应用程序将文件内容呈现给客户端节点。

在一个实施例中，在做出访问控制决定之前，访问控制服务器收集关于客户端节点的信息。在另一个实施例中，访问控制服务器将可执行文件传送给客户端节点，所述可执行文件包含与文件类型有关的应用程序的标识符和能够将文件内容呈现给客户端节点的应用程序服务器的标识符。在一个实施例中，在将文件内容呈现给客户端节点之前，访问控制服务器识别与文件类型有关的应用程序。在另一个实施例中，在将文件内容呈现给客户端节点之前，应用程序服务器识别与文件类型有关的应用程序。

另外，本发明涉及用于访问所转换的文件内容以实现增强的安全性从而提供基于政策的文档控制的方法和设备。

在一个方面中，本发明涉及准许访问资源的方法和设备。客户端节点请求访问资源。收集代理收集关于客户端节点的信息。政策机接收所收集的信息并且基于所接收的信息做出访问控制决定。转换服务器从政策机接收文件请求，将文件内容从原始格式转换成第二格式，并且将所转换的文件内容呈现给客户端节点。

在一个实施例中，政策机通过应用政策到所接收的信息来做出访问决定。在又一个实施例中，政策机传送收集代理给客户端节点。

在另一个方面中，本发明涉及用于准许访问资源的方法和设备。该设备包括政策机，该政策机包括两个部件。第一部件接收关于客户端节点的信息并且从该信息生成数据组。第二部件接收该数据组，并且基于所接收的数据组将可用于该客户端的资源枚举提供给第一部件。第一部件将所述资源的枚举呈现给客户端节点。

在一个实施例中，第一部件从收集代理接收信息。在一个实施例中，每个部件另外包括数据库。第一部件中的数据库存储条件。第二部件中的数据库存储政策。第一部件应用条件到所接收的信息并且第

二部件应用政策到所接收的数据组。

### 附图说明

本发明的这些和其它方面将从下面用于示例而并非用于限制本发明的具体描述和附图中变得易于明白，并且其中：

图 1A 是适合于实施本发明的示例性实施例的环境框图；

图 1B 和 1C 是描绘了用于本发明的计算机的实施例的框图；

图 1D 是计算机网络的实施例的框图，其中该网络提供准许访问网络资源的基于政策的系统；

图 2 是政策机的实施例的更具体的框图；

图 3 是描绘了由政策机基于所接收的关于客户端节点的信息做出访问控制决定所采取的步骤的一个实施例的流程图；

图 4 是计算机网络的实施例的框图，其中网络提供基于政策访问客户端节点的文件内容；

图 4B 是描绘了由应用程序服务器中心 (server farm) 提供文件内容给客户端节点所采取的步骤的一个实施例的流程图；

图 5 是计算机网络的实施例的框图，其中该网络准许访问所转换的资源内容；

图 6 是描绘了由转换服务器转换所请求的文件内容并且将该转换的内容呈现给客户端节点所采取的步骤的一个实施例的流程图；

图 7 是计算机网络的实施例的框图，其中在该计算机网络中提供了对多个应用程序会话的授权的远端访问；以及

图 7B 是描绘了通过会话服务器使客户端节点与其相关应用程序会话连接所采取的步骤的一个实施例的流程图。

### 具体实施方式

本发明的示例性实施例适用于分布式网络环境，其中远端用户请求访问内容。在讨论本发明的细节之前，讨论某些网络环境将是有帮助的，其中在该网络环境中可以应用本发明的示例性实施例。

图 1A 是适合于实施本发明的示例性实施例的环境框图。客户端节点 102 包括 web 浏览器 110 和应用程序 112a, 112b...112n。应用程序是处理数据来提供输出并且使用操作系统用于访问系统资源的任何

程序。典型应用程序包括：文字处理应用程序，比如由华盛顿州的雷蒙德的微软公司开发的 MICROSOFT WORD；电子制表软件程序，比如由微软公司开发的 MICROSOFT EXCEL；电子邮件程序，比如由微软公司开发的 MICROSOFT OUTLOOK 以及由犹他州 Provo 的 Novell 公司开发的 GROUPWISE；以及产品组，比如由加利福尼亚州 Mountain View 的 Sun Microsystems 开发的 STAR OFFICE。

内容服务器 126 包括内容文件 128 并且可以连接到分别保存附加内容文件 124 和 132 的数据存储器 122 和 130。本领域的技术人员将意识到，在不背离本发明范围的情况下保存内容文件的其它网络存储设备或文档贮藏库 (document repository) 也可以被联网到内容服务器 126。客户端节点 102 的用户可以使用 web 浏览器 110 从内容服务器 126 请求内容，来发送请求比如所描绘的超文本传输协议安全 (HTTPS) 请求 115，或者 HTTP (超文本传输协议)、FTP (文件传输协议) 请求，或者用于文件共享的操作，SMB (服务器管理块协议) 请求。

在许多实施例中，内容服务器 126、客户端节点 102 和代理服务器 120 被提供为由加利福尼亚州 Palo Alto 的 Hewlett-Packard 公司或德克萨斯州的 Round Rock 的戴尔 (Dell) 公司生产的那种类型的个人计算机或计算机服务器。图 1B 和 1C 描绘了在那些实施例中可用作内容服务器 126、代理服务器 120 或客户端节点 102 的典型计算机 100 的框图。如图 1B 和 1C 中所示，每个计算机 100 包括中央处理单元 102、和主存储器单元 104。每个计算机 100 还可以包括其它任选元件，比如一个或多个输入/输出设备 130a-130n (通常涉及使用参考数字 130)，以及与中央处理单元 102 进行通信的高速缓存器 140。

中央处理单元 102 是响应并且处理从主存储器单元 104 提取的指令的任何逻辑电路。在许多实施例中，中央处理单元由微处理器单元来提供，所述微处理器单元比如全部由加利福尼亚州的 Mountain View 的英特尔 (Intel) 公司生产的 8088、80286、80386、80486、奔腾处理器、高能奔腾、奔腾处理器 II、Celeron、或 Xeon 处理器；全部由伊利诺斯州的 Schaumburg 的摩托罗拉 (Motorola) 公司生产的 68000、68010、68020、68030、68040、PowerPC 601、PowerPC 604、PowerPC 604e、MPC603e、MPC603ei、MPC603ev、MPC603r、MPC603p、MPC740、MPC745、

MPC750、MPC755、MPC7400、MPC7410、MPC7441、MPC7445、MPC7447、MPC7450、MPC7451、MPC7455、MPC7457 处理器；由加利福尼亚州的 Santa Clara 的 Transmeta 公司生产的 Crusoe TM5800、Crusoe TM5600、Crusoe TM5500、Crusoe TM5400、Efficeon TM8600、Efficeon TM8300、或 Efficeon TM8620 处理器；全部由纽约州的 White Plains 的美国国际商用机器 (IBM) 公司生产的 RS/6000 处理器、RS64、RS64II、P2SC、POWER3、RS64 III、POWER3-II、RS64 IV、POWER4、POWER4+、POWER5 或 POWER6 处理器；或由加利福尼亚州的 Sunnyvale 的 AMD (Advanced Micro Devices) 公司生产的 AMD Opteron、AMD Athlon 64 FX、AMD Athlon、或 AMD Duron 处理器。

主存储器单元 104 可以是能够存储数据并且允许微处理器 102 直接访问任意存储位置的一个或多个存储器芯片，比如静态随机访问存储器 (SRAM)、或突发式 SRAM 或同步突发式 SRAM (BSRAM)、动态随机访问存储器 (DRAM)、快速页面模式 DRAM (FPM DRAM)、增强 DRAM (EDRAM)、可扩展数据输出 RAM (EDO RAM)、可扩展数据输出 DRAM (EDO DRAM)、突发可扩展数据输出 DRAM (BEDO DRAM)、增强 DRAM (EDRAM)、同步 DRAM (SDRAM)、JEDEC SRAM、PC100 SDRAM、双数据速率 SDRAM (DDR SDRAM)、增强 SDRAM (ESDRAM)、同步链路 DRAM (SLDRAM)、直接 Rambus DRAM (DRDRAM)、或铁电 RAM (FRAM)。

在图 1B 中所示的实施例中，处理器 102 通过系统总线 120 (下面将更具体地加以描述的) 与主存储器 104 进行通信。图 1C 描绘了计算机系统 100 的实施例，其中处理器通过存储器端口直接与主存储器 104 进行通信。例如，在图 1C 中，主存储器 104 可以是 DRDRAM。

图 1B 和图 1C 描绘了其中主处理器 102 通过有时称作“后方”总线的第二总线直接与高速缓存器 140 进行通信的实施例。在其它实施例中，主处理器 102 使用系统总线 120 与高速缓存器 140 进行通信。高速缓存器 140 典型地具有比主存储器 104 更快的响应时间并且典型地由 SRAM、BSRAM、或 EDRAM 提供。

在图 1B 中示出的实施例中，处理器 102 通过本地系统总线 120 与各种 I/O 设备 130 进行通信。各种总线可以用于连接中央处理单元 102 到 I/O 设备 130，所述总线包括 VESA VL 总线、ISA 总线、EISA 总线、微通道结构 (MCA) 总线、PCI 总线、PCI-X 总线、PCI-Express

总线、或 NuBus 总线。对于其中所述 I/O 设备为视频显示器的实施例，处理器 102 可以使用加速图形接口 (AGP) 来与显示器通信。图 1C 描绘了计算机系统 100 的实施例，其中主处理器 102 通过 HyperTransport (超高速传输)、快速 I/O (Rapid I/O)、或 InfiniBand(无限带宽) 直接与 I/O 设备 130b 进行通信。图 1C 还描绘了其中混合了本地总线和直接通信的实施例：处理器 102 使用本地互连总线与 I/O 设备 130a 通信同时与 I/O 设备 130b 直接进行通信。

多种 I/O 设备 130 可以呈现在计算机系统 100 中。输入设备包括键盘、鼠标、跟踪板、跟踪球、麦克风、以及写字板。输出设备包括视频显示器、扬声器、喷墨打印机、激光打印机、以及染料升华打印机 (dye-sublimation printer)。I/O 设备还可以提供用于计算机系统 100 的大容量存储器，比如硬盘驱动器、用于容纳软盘比如 3.5 英寸、5.25 英寸磁盘或 ZIP 磁盘的软盘驱动器、CD-ROM 驱动器、CD-R/RW 驱动器、DVD-ROM 驱动器、各种格式的磁带驱动器、以及 USB 存储器设备比如由加利福尼亚的洛杉矶的 Twintech Industry 公司生产的设备的 USB 闪速驱动线。

在另一个实施例中，I/O 设备 130 可以是系统总线 120 和外部通信总线之间的电桥 (bridge)，外部通信总线比如是 USB 总线、Apple Desktop Bus (苹果桌面总线)、RS-232 串行连接、SCSI 总线、火线 (FireWire) 总线、火线 800 总线、以太网总线、AppleTalk 总线、吉比特以太网总线、异步传输模式总线、HIPPI 总线、超 HIPPI 总线、SerialPlus 总线、SCI/LAMP 总线、光纤通道 (FibreChannel) 总线、或者串行连接小型计算机系统接口总线。

图 1B 和图 1C 中描绘的那种通用桌面计算机通常在操作系统的控制下工作，所述操作系统控制任务调度并且访问系统资源。其中，典型操作系统包括：由华盛顿州的雷蒙德的微软公司开发的 MICROSOFT WINDOWS；由加利福尼亚州的库珀蒂诺 (Cupertino) 的苹果计算机 (Apple Computer) 公司开发的 MacOS；由纽约州的 Armonk 的国际商用机器 (IBM) 公司开发的 OS/2；以及犹他州的盐湖城 (Salt Lake City) 的 Caldera 公司供销的免费获得的操作系统 Linux。

客户端节点 102 可以是任何个人计算机 (例如，286、386、486、奔腾、奔腾 II、Macintosh 计算机)、基于视窗的终端、网络计算机、

无线设备、信息设备、RISC Power PC、X 设备、工作站、微型计算机、主机计算机、个人数字助理、或具有基于视窗的桌面并且具有足够的永久存储器用于执行小型显示器显示节目的其它计算设备。显示器显示节目使用通过通信通道发送给它的命令和数据来呈现图形显示。所述客户端节点 102 支持的面向视窗的平台可以包括但不限于 WINDOWS 3.x、WINDOWS 95、WINDOWS 98、WINDOWS NT 3.51、WINDOWS NT 4.0、WINDOWS 2000、WINDOWS CE、MAC/OS、Java 以及 UNIX。客户端节点 102 可以包括可视显示器设备（例如，计算机监视器）、数据输入设备（例如，键盘）、用于存储下载的应用程序的永久或易失存储器（例如，计算机存储器）、处理器、以及鼠标。小型显示器显示节目的执行允许客户端节点 102 参与分布式计算机系统模型（即，基于服务器的计算模型）。

对于其中客户端节点 102 为移动设备的实施例，所述设备可以是 JAVA 使能的蜂窝电话，比如全部由伊利诺斯州的 Schaumburg 的摩托罗拉 (Motorola) 公司生产的 i50sx、i55sr、i58sr、i85s、i88s、i90c、i95c1、或 im11000；由日本京都的 Kyocera 生产的 6035 或 7135；或者韩国汉城的三星电子有限公司生产的 i300 或 i330。在其中客户端节点 102 为移动的其它实施例中，它可以是在 PalmOS 操作系统控制下工作的个人数字助理 (PDA)，比如全部由加利福尼亚州的 Milpitas 的 palmOne 公司生产的 Tungsten W、VII、VIIx、i705。在另外的实施例中，客户端节点 102 可以是在 PocketPC 操作系统控制下工作的个人数字助理 (PDA)，比如全部由加利福尼亚州的 Palo Alto 的 Hewlett-Packard 公司生产 iPAQ 4155、iPAQ 5555、iPAQ 1945、iPAQ 2215、以及 iPAQ 4255；由加利福尼亚州的 Walnut 的 ViewSonic 公司生产的 ViewSonic V36；或者由纽约州的纽约的东芝美国公司生产的东芝 PocketPC e405。在又一个实施例中，客户端节点是组合 PDA/电话设备，比如全部由加利福尼亚州的 Milpitas 的 palmOne 公司生产的 Treo 180、Treo 270 或 Treo 600。在又一个实施例中，客户端节点 102 为在 PocketPC 操作系统控制下工作的蜂窝电话，比如由摩托罗拉公司生产的 MPx200。

现在参照图 1D，描绘了根据本发明构建的计算机网络 100 的一个实施例，其包括客户端节点 102、收集代理 104、政策机 106、政策数

数据库 108、应用程序服务器中心 114、以及应用程序服务器 116。尽管在图 1D 所示的实施例中仅描绘了一个客户端节点 102、收集代理 104、政策机 106、应用程序服务器中心 114、以及应用程序服务器 116，应当理解本系统可以提供这些部件中任意一种或每一种的多个。例如，在一个实施例中，系统 100 包括多个逻辑分组的应用程序服务器 116，其中的每一个可用于代表所述客户端节点 102 执行应用程序。在这些实施例中，该逻辑组服务器可以称作“服务器中心”。在这些实施例的某些实施例中，服务器可以在地理上被分散。

概言之，当客户端节点 102 传送请求 110 到政策机 106 用于访问资源时，收集代理 104 与客户端节点 102 进行通信，取回关于客户端节点 102 的信息，并且传送客户端节点信息 112 到政策机 106。政策机 106 通过将来自政策数据库 108 的政策应用到所接收的信息 112 做出访问控制决定。

更具体地，客户端节点 102 传送用于资源的请求 110 到政策机 106。在某些实施例中，客户端节点 102 通过网络连接传送请求 110。网络可以是局域网 (LAN)、城域网 (MAN)、或者广域网 (WAN) 比如互联网。客户端节点 102 和政策机 106 可以通过多种连接而连接到网络，所述连接包括标准电话线、LAN 或 WAN 链路 (例如，T1、T3、56kb、X.25)、宽带连接 (ISDN、帧中继、ATM)、以及无线连接。客户端节点 102 和政策机 106 之间的连接可以使用多种数据链路层通信协议 (例如，TCP/IP、IPX、SPX、NetBIOS、NetBEUI、SMB、Ethernet (以太网)、ARCNET、光纤分布式数据接口 (FDDI)、RS232、IEEE 802.11、IEEE 802.11a、IEEE 802.11b、IEEE 802.11g 以及直接异步连接)。

一旦接收到请求，政策机 106 通过收集代理 104 发起信息收集。收集代理 104 收集关于客户端节点 102 的信息并且将信息 112 传送给政策机 106。

在一些实施例中，收集代理 104 收集并且通过网络连接传送信息 112。在一些实施例中，收集代理 104 包括字节码，比如以字节码编程语言 JAVA 编写的应用程序。在一些实施例中，收集代理 104 包括至少一个脚本。在那些实施例中，收集代理 104 通过在客户端节点 102 上运行至少一个脚本来收集信息。在一些实施例中，收集代理包括在客户端节点 102 上的 Active X 控件。Active X 控件是一种实现一组

接口的专用 COM (组件对象模型) 对象, 该接口使得其能够看起来和做起来像一种控件。

在一些实施例中, 收集代理 104 在客户端节点上执行。在其它实施例中, 收集代理 104 位于政策机 106 上。在又一些实施例中, 收集代理 104 位于服务器上。在其它实施例中, 政策机 106 位于该服务器上。在这些实施例的某些实施例中, 收集代理 104 位于政策机 106 和该服务器上。

在一个实施例中, 政策机 106 传送收集代理 104 给客户端节点 102。在一个实施例中, 在收集代理 104 已经传送信息 112 给政策机 106 之后, 政策机 106 需要收集代理 104 的第二次执行。在这个实施例中, 政策机 106 可以具有不足信息 112 来判定客户端节点 102 是否满足特定条件。在其它实施例中, 政策机 106 响应于所接收的信息 112 要求收集代理 104 的多次执行。

在一些实施例中, 政策机 106 传送指令给收集代理 104 确定收集代理 104 收集的信息类型。在那些实施例中, 系统管理员可以配置从政策机 106 传送到收集代理 104 的指令。这对所收集的信息类型提供了更大控制。由于对于所收集的信息的类型提供了更大控制, 这还扩展了政策机 106 可以做出的访问控制决定的类型。收集代理 104 收集信息 112, 该信息包括但不限于客户端节点的机器 ID、操作系统类型、操作系统补丁的存在、被安装的网卡的 MAC 地址、客户端设备上的数字水印、有效目录 (active directory) 中的从属关系、病毒扫描软件 (virus scanner) 的存在、个人防火墙的存在、HTTP 报头、浏览器类型、设备类型、网络连接信息、以及授权证书。

在一些实施例中, 设备类型是个人数字助理。在其它实施例中, 设备类型是蜂窝电话。在其它实施例中, 设备类型是膝上型计算机。在其它实施例中, 设备类型是桌上型计算机。在其它实施例中, 设备类型是互联网公用电话亭 (Internet kiosk)。

在一些实施例中, 数字水印包括数据嵌入。在一些实施例中, 水印包括插入文件中的数据模式以提供关于该文件的源信息。在其它实施例中, 水印包括数据散列文件以提供篡改检测。在其它实施例中, 水印提供关于所述文件的版权信息。

在一些实施例中, 网络连接信息与带宽能力有关。在其它实施例

中，网络连接信息与互联网协议地址有关。在又一些实施例中，网络连接信息包含互联网协议地址。在一个实施例中，网络连接信息包括网络区域（network zone），该网络区域识别登录上网代理，客户端节点提供认证证书给该登录上网代理。

在一些实施例中，授权证书包括多种类型的认证信息，包括但不限于用户名、客户端名、客户端地址、口令、PIN、语音采样、一次性口令、生统统计数据（biometric data）、数字证书、标签等等及其组合。在接收到所收集的信息 112 之后，政策机 106 基于所接收的信息 112 做出访问控制决定。

现在参照图 2，它是政策机 200 的一个实施例的框图，包括第一部件 202 和第二部件 210，其中第一部件 202 包括条件数据库 204 和登录上网代理 206，第二部件 210 包括政策数据库 212。第一部件 202 将来自条件数据库 204 的条件应用到所接收的关于客户端节点 102 的信息并且判定所接收的信息是否满足条件。

在一些实施例中，第一部件 202 和第二部件 210 逻辑上独立但物理上不独立。在一些实施例中，第一部件 202 和第二部件 210 逻辑和物理上独立。在一些实施例中，条件数据库 204 位于第一部件 202 上。在其它实施例中，条件数据库 204 位于第二部件 210 上。

在一些实施例中，条件可以要求客户端节点 102 执行特定操作系统来满足该条件。在一些实施例中，条件可以要求客户端节点 102 执行特定操作系统补丁以满足该条件。在又一些实施例中，条件可以要求客户端节点 102 提供用于每个被安装的网卡的 MAC 地址以满足该条件。在一些实施例中，条件可以要求客户端节点 102 表明在特定有效目录中的从属关系以满足该条件。在另外的实施例中，条件可以要求客户端节点 102 执行病毒扫描软件以满足条件。在其它实施例中，条件可以要求客户端节点 102 执行个人防火墙以满足该条件。在一些实施例中，条件可以要求客户端节点 102 包括特定设备类型以满足该条件。在其它实施例中，条件可以要求客户端节点 102 建立特定类型的网络连接以满足该条件。

如果所接收的信息满足条件，那么第一部件 202 在数据组 208 中为那个条件存储标识符。在一个实施例中，如果信息使得条件为真，那么所接收的信息满足条件。例如，条件可以要求安装特定操作系统。

如果客户端节点 102 具有那个操作系统，那么该条件为真并且满足。在另外的实施例中，如果信息使得条件为假，则所接收的信息满足条件。例如，条件可以针对 spyware（间谍软件）是否存在客户端节点 102 上。如果客户端节点 102 不包含间谍软件，则条件为假并且满足。

在一些实施例中，登录上网代理 206 位于政策机 200 之外。在其它实施例中，登录上网代理 206 位于政策机 200 上。在一个实施例中，第一部件 202 包括登录上网代理 206，该登录上网代理 206 发起关于客户端节点 102 的信息收集。在一些实施例中，登录上网代理 206 进一步包括数据存储器。在这些实施例中，数据存储器包括收集代理可以收集信息的条件。这个数据存储器不同于条件 DB 204。

在一些实施例中，登录上网代理 206 通过执行收集代理 104 发起信息收集。在其它实施例中，登录上网代理 206 通过传送收集代理 104 给客户端节点 102 发起信息收集用于在客户端节点 102 上执行。在又一些实施例中，登录上网代理 206 在接收信息 112 之后发起另外的信息收集。在一个实施例中，登录上网代理 206 也接收信息 112。在这个实施例中，登录上网代理 206 基于所接收的信息 112 生成数据组 208。在一些实施例中，登录上网代理 206 通过将来自数据库 204 的条件应用到从收集代理 104 接收的信息来生成数据组 208。

在另外的实施例中，第一部件 202 包括多个登录上网代理 206。在这个实施例中，所述多个登录上网代理 206 中的至少一个位于每个网络域上，客户端节点 102 可以从所述每个网络域传送资源请求。在这个实施例中，客户端节点 102 传送资源请求给特定登录上网代理 206。在一些实施例中，登录上网代理 206 将客户端节点 102 从其访问登录上网代理 206 的所述网络域传送给政策机 200。在一个实施例中，客户端节点 102 从其访问登录上网代理 206 的网络域被称作客户端节点 102 的网络区域。

条件数据库 204 存储第一部件 202 应用到所接收信息的条件。政策数据库 212 存储第二部件 210 应用到所接收数据组的政策。在一些实施例中，条件数据库 204 和政策数据库 212 在 ODBC 相容数据库中存储数据。例如，条件数据库 204 和政策数据库 212 可以被提供为由加利福尼亚州的 Redwood Shores 的 Oracle 公司开发的 ORACLE 数据库。在其它实施例中，条件数据库 204 和政策数据库 212 可以是华盛顿州

的雷蒙德的微软公司开发的 Microsoft ACCESS 数据库或 Microsoft SQL 服务器数据库。

在第一部件 202 将所接收的信息应用到条件数据库 204 中的每个条件之后，第一部件传送数据组 208 到第二部件 210。在一个实施例中，第一部件 202 仅传送数据组 208 到第二部件 210。因此，在这个实施例中，第二部件 210 不接收信息 112，仅接收满足条件的标识符。第二部件 210 接收数据组 208 并且基于数据组 208 中所识别的条件通过应用来自政策数据库 212 的政策做出访问控制决定。

在一个实施例中，政策数据库 212 存储应用到所接收的信息 112 的政策。在一个实施例中，存储在政策数据库 212 中的政策至少部分地由系统管理员指定。在另外的实施例中，用户指定存储在政策数据库 212 中的至少一些政策。用户指定的一个或多个政策被存储为优先选择。政策数据库 212 可以被存储在易失或非易失存储器中或者例如通过多个服务器分配。

在一个实施例中，只有当满足一个或多个条件，政策才允许访问资源。在另外的实施例中，政策允许访问资源但是禁止传送资源到客户端节点 102。存储在政策数据库 212 中的政策之一可能要求或者禁止自动连接到断开的应用程序会话。又一政策可能做出发生在客户端节点 102 上的连接，该连接请求在安全网络中进行访问。另一政策可能要求或者禁止自动连接到当前被连接到不同客户端节点 102 的有效应用程序会话。另一政策可能仅允许在接收到用户准许之后连接到应用程序会话。另一政策可能仅在断开之后预定时间允许连接。又一个政策可能仅允许连接到包括特定应用程序的应用程序会话。一种政策可能允许仅仅观看请求文件的转换内容。一种政策可能允许仅仅观看请求文件的 HTML 版本。在一些实施例中，提供访问资源同时防止文件下载到客户端节点 102。这可能以多种方式来完成，包括：转换文件内容为仅阅读器格式、转换文件内容为 HTML，用于使用 web 浏览器观看、使用相关的文件类型来使用服务器中心的服务器拥有的应用程序，而不是使用客户端节点 102 拥有的应用程序打开文件、或者通过使用在美国专利申请序列号 10/931405 中描述的那种系统，该申请的内容在此作为参考被结合进来。

在上面的一些实施例中，该方法和设备提供私有信息的文档保

护。在这些实施例中，客户端节点不能访问联网资源除非政策机 106 准许客户端节点 102 允许访问资源。在这些实施例之一中，政策机 106 为单个外露的网络元件，用来保证客户端节点 102 必须访问政策机 106 以便访问联网资源。在这些实施例的另一个实施例中，用于在政策机 106 之后访问联网资源的 URL 被重新写入来防止客户端节点 102 的直接访问。在上面其它实施例中，所述方法和设备增强客户端节点访问资源的能力，该资源用别的方式是不可访问的。在上面的一些实施例中，所述方法和设备提供私有信息的保护和增强的客户端节点能力。

现在参照图 3，流程图描绘了由政策机 106 基于所接收的关于客户端节点 102 的信息做出访问控制决定所采取的步骤的一个实施例。一旦接收到所收集的关于客户端节点 102 的信息（步骤 350），政策机 106 基于所述信息生成数据组（步骤 352）。在一些实施例中，政策机 106 从收集代理 104 请求关于客户端节点 102 的另外信息。在这些实施例中，政策机 106 要求在客户端节点 102 上不止一次执行收集代理 104。在那些实施例中，政策机 106 在接收到附加的请求信息之后生成数据组 108。在这些实施例中，政策机 106 可以具有不足的信息 112 来判定客户端节点 102 是否满足特定条件。在这些实施例的其它实施例中，条件可以是不确定的。在其中条件是不确定的一些实施例中，收集代理不能收集满足该条件所要求的信息。

数据组 208 包含由所接收信息 112 所满足的每个条件的标识符。接着，政策机 106 将政策应用到数据组 208 中的每个所识别的条件。那个应用程序产生客户端节点 102 可以访问的资源的枚举（步骤 354）。在一个实施例中，资源包括私有数据。在一些实施例中，资源包括 web 网页。在其它实施例中，资源包括文字处理文档。在又一些实施例中，资源包括电子制表软件。在一些实施例中，所述枚举包括仅客户端节点 102 可以访问的资源的子组。政策机 106 然后将所述枚举呈现给客户端节点 102。在一些实施例中，政策机 106 创建用于将所述枚举呈现给客户端节点的超文本链接标示语言（HTML）文档。

现在参照图 4，描绘了根据本发明构建的计算机网络 400 的一个实施例，其包括客户端节点 402、收集代理 404、访问控制服务器 406、政策数据库 408、应用程序服务器中心 414、第一应用程序服务器 416、应用程序数据库 418、第二应用程序服务器 420、以及第二应用程序

数据库 422。在一些实施例中，存在将客户端节点 402 所位于的网络与访问控制服务器 406 和应用程序服务器中心 414 所位于的网络分隔的网络边界。

概言之，当客户端节点 402 传送访问资源的请求 410 给访问控制服务器 406 时，收集代理 404 与客户端节点 402 进行通信，取回关于客户端节点 402 的信息，并且传送客户端节点信息 412 至访问控制服务器 406。在一个实施例中，在政策机 106 向客户端节点 402 呈现可用资源的枚举之后，客户端节点 402 传送请求 410。访问控制服务器 406 通过将来自政策数据库 408 的政策应用到所接收的信息 412 做出访问控制决定。最后，访问控制服务器 406 传送文件类型给应用程序服务器中心 414 用于将文件内容呈现给客户端节点 402。省略了计算机网络 400 的附加部件并且其将在图 4B 中进一步加以描述。

现在参照图 4B，流程图描绘了访问控制服务器 406 和应用程序服务器中心 414 提供文件内容给客户端节点 402 所采取的步骤的一个实施例。应用程序服务器中心 414 的一部分是应用程序服务器 416。

在一个实施例中，一旦访问控制服务器 406 决定准许客户端节点 402 访问所请求的文件，则访问控制服务器 406 确定所请求的文件的文件类型（步骤 452）。在其它实施例中，应用程序服务器 416 确定所请求的文件的文件类型。在又一些实施例中，除了应用程序服务器 416 或者访问控制服务器 406 之外的服务器。在一些实施例中，确定文件类型的服务器必须首先取回所请求的文件。在那些实施例的一些实施例中，文件位于网络边界 424 的与确定文件类型的服务器同一侧。在那些实施例的其它实施例中，文件位于网络边界 424 的与客户端节点 402 同一侧。在这些实施例中，所述方法和设备增强了客户端节点访问资源的能力，该资源用别的方式是不可访问的，但是它们不提供私有信息的文档保护。

在一些实施例中，网络边界 424 物理上分割至少两个网络。在其它实施例中，网络边界 424 逻辑上分割至少两个网络。在一个实施例中，网络边界 424 是防火墙。

在一个实施例中，文件扩展名是文件类型并且确定文件类型的服务器通过从文件中提取文件扩展名来做到这一点。在另一个实施例中，资源分支（resource fork）是文件类型。在确定文件类型之后，

确定文件类型的服务器传送文件类型给应用程序服务器中心 414 用于取回和呈现给客户端节点 402 (步骤 454)。

应用程序服务器 416 从访问控制服务器 406 接收文件类型 (步骤 456)。在一些实施例中, 应用程序服务器 416 识别与那个文件类型有关的应用程序。在其它实施例中, 访问控制服务器 406 识别与那个文件类型有关的应用程序。在又一些其它实施例中, 除了访问控制服务器 406 或应用程序服务器 416 之外的服务器识别与那个文件类型有关的应用程序。

在一个实施例中, 识别与文件类型有关的应用程序的服务器查询应用程序数据库 418 来取回用于应用程序的标识符。在一些实施例中, 应用程序数据库 418 是登记文件。在其中应用程序服务器 416 或单独服务器基于文件类型识别应用程序类型的实施例中, 识别服务器于是传送应用程序的所述标识符给访问控制服务器 406。在一些实施例中, 识别服务器通过网络连接传送标识符给访问控制服务器 406。

在一些实施例中, 访问控制服务器 406 或单独服务器都不需要传送文件类型给应用程序服务器 416, 以确定相关应用程序的标识符。在这些实施例之一中, 应用程序服务器 416 传送所拥有的应用程序列表和与那些应用程序有关的文件类型给访问控制服务器 406。在这些实施例中, 访问控制服务器 406 从所传送的列表中取回与文件类型有关的应用程序的标识符。

当访问控制服务器 406 接收应用程序的标识符时, 访问控制服务器 406 创建并且传送可执行文件给客户端节点 402 (步骤 458)。在一些实施例中, 可执行文件包含应用程序的标识符。在一些实施例中, 可执行文件包含将文件内容呈现给客户端节点 402 的应用程序服务器中心 414 中的应用程序服务器的标识符。在一些实施例中, 使用文件类型识别应用程序的同一应用程序服务器 416 将文件内容呈现给客户端节点 402。在其它实施例中, 第二应用程序服务器 420 将文件内容呈现给客户端节点 402。在一个实施例中, 可执行文件包含应用程序的标识符和将文件内容呈现给客户端节点 402 的应用程序服务器中心 414 中的应用程序服务器的标识符。在一些实施例中, 可执行文件使得客户端节点 402 能够使用表示层协议, 比如来自佛罗里达的 Fort Lauderdale 的 Citrix Systems 公司的独立计算结构 (ICA) 协议与所

识别的服务器连接。在其它实施例中，可执行文件使得客户端节点 402 能够使用微软公司开发的远端桌面协议（RDP），与所识别的服务器连接。在其它实施例中，表示层协议被封装在较高层的协议中。

客户端节点 402 从访问控制服务器 406 接收可执行文件。客户端节点 402 连接到在可执行文件中识别的应用程序服务器 416（步骤 460）。在一个实施例中，客户端节点 402 使用 ICA 协议连接到所识别的应用程序服务器 416。在另一个实施例中，客户端节点 402 使用 RDP 连接到所识别的应用程序服务器 416。

应用程序服务器 416 选择呈现文件内容的格式（步骤 464）。在其它实施例中，访问控制服务器 406 识别用于呈现文件内容的格式。在那些实施例中，访问控制服务器 406 可应用政策来识别可用格式。在一些实施例中，应用程序服务器 416 基于所接收的关于客户端节点 402 的信息选择格式。在其它实施例中，应用程序服务器 416 通过将政策应用到所接收的信息来选择格式。

应用程序服务器 416 接受客户端节点 402 连接并且取回所请求的文件（步骤 466）。在一个实施例中，应用服务器 416 从 web 服务器取回文件。在另一个实施例中，应用程序服务器 416 从文件服务器取回文件。在又一个实施例中，所取回的文件是电子邮件的附件。在这个实施例中，应用程序服务器 416 从电子邮件服务器中取回文件。在一些实施例中，邮件服务器是 Lotus 邮件服务器。在其它实施例中，邮件服务器是 Outlook 邮件服务器或者 Outlook Web Access 邮件服务器。

应用程序服务器 416 通过连接将文件内容呈现给客户端节点 402（步骤 468）。在一个实施例中，所呈现的文件内容包含电子邮件附件。

参照图 5，描绘了根据本发明构建的计算机网络 500 的一个实施例，该计算机网络包括客户端节点 502，收集代理 504，政策机 506，第一部件 508，第二部件 512，条件数据库 510，政策数据库 512，转换服务器 516，和存储元件 518。概言之，当客户端节点 502 从政策机 506 传送用于访问资源的请求 522 时，收集代理 504 与客户端节点 502 进行通信，取回关于客户端节点 502 的信息，并且传送客户端节点信息 512 至政策机 506。政策机 506 做出访问控制决定，如上面图

3 中所讨论的。一旦政策机 506 决定准许客户端节点 502 访问所请求的文件，则政策机 506 传送该请求至转换服务器 516 用于转换和呈现给客户端节点 502。

更具体地，政策机 506 从客户端节点 502 接收用于所转换的文件内容的请求。在一个实施例中，政策机 506 识别能够将所转换的文件内容呈现给客户端节点 502 的转换服务器 516。在一些实施例中，转换服务器 516 能够呈现转换的文件内容，因为它包含之前转换的内容的拷贝。在其它实施例中，转换服务器 516 能够呈现转换的文件内容，因为它当前有能力转换文件内容。

在一个实施例中，政策机 506 通过查询一个存储元件 518 以决定是否转换服务器 516 之前转换了文件内容来识别转换服务器 516。在那个实施例中，政策机 506 传送由存储元件 518 识别的转换服务器 518 的标识符给客户端节点 502。在其它实施例中，没有任何转换服务器 516 之前转换内容。在那些实施例中，政策机 506 而是识别当前能够转换文件内容的转换服务器 516 并且传送客户端节点 502 的请求至那个转换服务器 516。

在其它实施例中，除了政策机 506 之外的服务器识别能够将所转换的文件内容呈现给客户端的转换服务器 516。在这些实施例的一些实施例中，同一服务器还向转换服务器 516 传送将文件呈现给客户端的请求。在这些实施例的一些实施例中，识别有能力的转换服务器 516 的同一服务器通过代理服务器路由并且传送所述请求给转换服务器 516。

在一个实施例中，转换服务器 516 接收来自政策机 506 的请求用于转换所请求文件的内容并且呈现给客户端节点 502。在另一实施例中，转换服务器 516 接收来自除了政策机 506 之外的服务器的请求。转换服务器 516 取回文件并且将内容从原始格式转换成第二格式。转换服务器 516 然后接受来自客户端节点 502 的连接并且呈现所转换的文件内容，如果所述内容先前没有转换的话则转换所述内容。最后，转换服务器 516 将转换文件内容的服务器的标识符和文件的标识符写入存储元件 518。

现在参照图 6，流程图描绘了由转换服务器 516 转换所请求的文件内容并且将该转换的内容呈现给客户端节点 502 所采取的步骤的一

个实施例。

转换服务器 516 接收所请求文件的内容的转换请求并且呈现给客户端节点 502 (步骤 600)。在一个实施例中, 转换服务器 516 通过网络连接接收这个请求。

转换服务器 516 将所请求的文件内容从原始格式转换为第二格式 (步骤 602)。在一个实施例中, 转换服务器 516 使用规则表示将文件内容从原始格式转换为第二格式用于呈现在客户端上。在另一实施例中, 转换服务器 516 将文件内容从原始格式转换成第二格式, 其包含格式转换工具。在另一实施例中, 转换服务器 516 将文件内容从原始格式转换成 HTML。在另一实施例中, 转换服务器 516 将文件内容从原始格式转换成第二格式, 其中第二格式使得能够在个人数字助理上呈现。在另一实施例中, 转换服务器 516 将文件内容从原始格式转换成第二格式, 其中第二格式使得能够在蜂窝电话上呈现。在另一实施例中, 转换服务器 516 将文件内容从原始格式转换为第二格式, 其中第二格式使得能够在膝上型计算机上呈现。在另一实施例中, 转换服务器 516 将文件内容从原始格式转换为第二格式, 其中第二格式使得能够在互联网公用电话亭上呈现。

转换服务器 516 将关于所述转换的识别信息写入存储元件 518 (步骤 604)。在一个实施例中, 识别信息包括转换服务器 516 的标识符以及所转换的文件的标识符。在一些实施例中, 识别信息包括临时文件, 该临时文件包含所转换的文件内容。在那些实施例中, 存储元件 518 用作所转换的文件内容的全局高速缓存器。

在政策机 506 识别能够呈现用于客户端节点 502 的所转换的文件内容的转换服务器 516 之后, 政策服务器 506 传送转换服务器 516 的标识符给客户端节点 502。客户端节点 502 接收标识符并且连接到转换服务器 516。转换服务器 516 接受所述连接并且通过该连接将所请求文件的转换内容呈现给客户端节点 502 (步骤 606)。在一个实施例中, 转换服务器 516 在呈现给客户端节点 502 之后保留所请求文件的转换内容。

参照图 7, 描绘了根据本发明构建的计算机网络 700 的一个实施例, 其包括第一客户端节点 702、收集代理 704、政策机 706、政策数据库 708、条件数据库 710、第二客户端节点 716、会话服务器 720、

所存储的应用程序数据库 722、应用程序服务器中心 724、第一应用程序服务器 726、第一数据库 728、第二应用程序服务器 730、以及第二数据库 732。概言之，当第一客户端节点 702 传送访问资源的请求 712 到访问控制服务器 706 时，收集代理 704 与客户端节点 702 进行通信，取回关于客户端节点 702 的信息，并且传送客户端节点信息 714 给政策机 706。政策机 706 做出访问控制决定，如上面图 3 中所讨论的。最后，会话服务器 720 在客户端节点 702 和与客户端节点 702 有关的多个应用程序会话之间建立连接。计算机网络 700 的附加部件被省略并且其将在图 7B 中进一步加以描述。

现在参照图 7B，流程图描绘了由会话服务器 720 使客户端节点 702 与其相关应用程序会话连接所采取的步骤的一个实施例。会话服务器 720 从政策机 706 接收关于客户端节点 702 的包含政策机 706 做出的访问控制决定的信息。在一个实施例中，该信息还包括客户端节点信息 714。

在一些实施例中，政策机 706 识别已经与客户端节点 702 有关的多个应用程序会话。在其它实施例中，会话服务器 720 识别与客户端节点 702 有关的所存储的应用程序会话。在这些实施例的一些实施例中，一接收到来自政策机 706 的信息，会话服务器 720 自动识别所存储的应用程序会话。在一个实施例中，所存储的应用程序数据库 722 位于会话服务器 720 上。在另一实施例中，所存储的应用程序数据库 722 位于政策机 706 上。

所存储的应用程序数据库 722 包含与执行应用程序会话的应用程序服务器中心 724 中的多个服务器有关的数据。在一些实施例中，识别与客户端节点 702 有关的应用程序会话要求查阅与执行应用程序会话的一个或多个服务器有关的存储数据。在这些实施例的一些实施例中，会话存储器 720 查阅与执行应用程序会话的一个或多个服务器有关的存储数据。在这些实施例的其它实施例中，政策机 706 查阅与执行应用程序会话的一个或多个服务器有关的存储数据。在一些实施例中，第一应用程序会话运行在第一应用程序服务器 726 上并且第二应用程序会话运行在第二应用程序服务器 730 上。在其它实施例中，所有应用程序会话运行在应用程序服务器中心 724 中的单个应用程序服务器上。

会话服务器 720 包括与由用户发起的应用程序会话有关的信息。会话服务器可以被存储在易失或非易失存储器中，或者例如通过多个服务器分配。表格 7-1 示出了包括在所示例性会话服务器 720 的一部分中的数据。

表格 7-1

应用程序会话	应用程序会话 1	应用程序会话 2	应用程序会话 3
用户 ID	用户 1	用户 2	用户 1
客户端 ID	第一客户端		第一客户端
客户端地址	172.16.0.50		172.16.0.50
状态	有效	断开	有效
应用程序	文字处理器	数据库	电子制表软件
处理序号	1	3	2
服务器	服务器 A	服务器 A	服务器 B
服务器地址	172.16.2.55	172.16.2.55	172.16.2.56

表格 7-1 中的示例性会话服务器 720 包括使每个应用程序会话与发起应用程序会话的用户相关联的数据，客户端计算机 702 或 716 的标识，如果有的话，当前用户从其被连接到服务器 726、以及那个客户端计算机 702a 或 716 的 IP 地址。所示例的会话服务器 720 还包括每个应用程序会话的状态。应用程序会话状态可以例如为“有效”（指用户被连接到应用程序会话）或者“断开”（指用户没有连接到应用程序会话）。在可替换的实施例中，应用程序会话状态还可以被设置为“执行-断开”（指用户已经从所述应用程序会话断开，但是应用程序会话中的应用程序仍旧执行），或者“停止-断开”（指用户断开并且应用程序会话中的应用程序没有执行，但是它们的工作状态在断开之前立即被保存）。会话服务器 720 进一步存储表示在每个应用程序会话中执行的应用程序 116 和表示在服务器上每个应用程序处理的数据的信息。在其中服务器 726 为服务器中心 724 的一部分的实施例中，会话服务器 720 至少为动态存储器的一部分，并且还包括表格 1 的最后两行中的数据，该数据表示每个应用程序正在服务器中心中的哪个服务器上执行，以及那个服务器的 IP 地址。在可替换的实施例中，会话服务器 720 包括在每个应用程序会话中的每个应用程序的状态指示符。

例如，在表格 7-1 的例子中，存在三个应用程序会话，即应用程序会话 1、应用程序会话 2、和应用程序会话 3。应用程序会话 1 与用户 1 相关联，该用户当前使用终端 1。终端 1 的 IP 地址为 152.16.2.50。应用程序会话 1 的状态为有效，并且在应用程序会话 1 中，正在执行文字处理程序。文字处理程序在服务器 A 上执行，作为处理序号 1。服务器 A 的 IP 地址是 152.16.2.55。表格 1 中的应用程序会话 2 是断开的应用程序会话 118 的例子。应用程序会话 2 与用户 2 相关联，但是应用程序会话 2 没有连接到客户计算机 702a 或 716。应用程序会话 2 包括在服务器 A 上执行的数据库程序，服务器 A 的 IP 地址为 152.16.2.55，处理序号为 3。应用程序会话 3 是用户如何与在不同服务器 726 上工作的应用程序会话交互的例子。应用程序会话 3 与应用程序会话 1 一样也与用户 1 相关联。应用程序会话 3 包括在服务器 B 上执行的电子制表软件程序，服务器 B 的 IP 地址是 152.16.2.56，处理序号为 2，而包括在应用程序会话 1 中的应用程序会话在服务器 A 上执行。

在一个实施例中，会话服务器 720 被配置来接收断开请求来断开与客户端节点 702 有关的应用程序会话并且响应于所述请求这么做来断开应用程序会话。会话服务器 720 在从应用程序会话断开客户端节点 702 之后继续执行应用程序会话。在这个实施例中，会话服务器 720 访问所存储的应用程序数据库 722 并且更新与每个断开应用程序会话有关的数据记录，这样该记录表示与客户端节点 702 有关的应用程序会话是断开的。

由不完善网络连接和用户自己不能终止它们的应用程序会话引起的应用程序会话的无意识终止可以给用户带来麻烦。本发明的一个实施例通过区分断开（其被当作用户没有完成与应用程序会话一起工作来处理）与终止（其被假设为有意结束应用程序会话）并且通过将应用程序会话与相对于客户端节点的用户相关，限制这些麻烦。当用户使用工作在应用程序会话中的应用程序结束时，用户可以终止应用程序会话。终止通常包括表示服务器应当不再保持应用程序会话的用户肯定输入。这样的肯定用户输入可以包括从菜单选择“退出”选项，点击图标等等。响应于接收终止请求的会话服务器 720，暂停那个应用程序会话中的应用程序会话和任何应用程序的执行。在一个实施例

中，与应用程序会话有关的数据也从所存储的应用程序数据库 722 中移除。

另一方面，不管是有意还是无意的断开，不会引起应用程序会话的终止。由于工作在应用程序会话中的一个或多个应用程序在服务器 720 上执行，到第一客户端节点 702 的连接通常不必继续执行应用程序，并且在一个实施例中，应用程序可以继续执行同时等待用户连接。在可替换的实施例中，一旦断开用户，会话服务器 720 停止工作在应用程序会话中的应用程序的执行。即，会话服务器 720 停止应用程序的进一步执行，并且会话服务器 720 存储应用程序的工作状态以及应用程序正在处理的任何数据。在另一实施例中，在用户断开之后，会话服务器 720 可以选择地停止特定应用程序的执行。例如，在一个实施例中，会话服务器 720 继续执行应用程序一个固定时间段，并且如果用户不能在那个时间段内连接，那么会话服务器 720 停止该应用程序。在另一实施例中，会话服务器 720 不使用任何用户输入停止不能继续执行的特定应用程序会话。在每个上面所述的实施例中，如果第一客户端节点 702 的用户从服务器 726 断开并且然后连接到服务器 726 同时操作第一客户端节点 702、第二客户端节点 716、或第三客户端计算机，则会话服务器 720 可以连接由用户操作的客户端计算机到一个或多个先前发起的与用户有关的未终止的一个或多个应用程序会话，并且重新发起任何停止的应用程序的执行。

在一个实施例中，会话服务器 720 检测到断开。用户可以有意和手工命令服务器从用户正在与之通信的客户端节点 702 或 716 断开应用程序会话。例如，在一个实施例中，应用程序会话提供用户可以选择的用于断开（与上面的终止有所区别）的菜单选项。会话服务器 720 还可以检测无意断开。例如，在一个实施例中，会话服务器 720 识别何时传送到客户端节点 702 或 716 的预定数量的数据分组还没有由客户端节点 702 或 716 确认。在另一实施例中，客户端节点 702 或 716 定期传送信号给服务器 726 来确认连接仍旧保持原样。如果会话服务器 720 检测到来自客户端节点 702 或 716 的预定数量的预期确认信号还没有到达，那么会话服务器 720 确定客户端节点 702 或 716 已经断开。如果会话服务器 720 检测到用户已经从应用程序会话有意或无意地断开，那么与断开的应用程序会话有关的会话服务器 720 中的项目

被修改来反映该断开。

在接收到认证信息之后，会话服务器 720 查阅所存储的应用程序数据库 722 来识别与用户有关但连接到不同客户端节点比如举例来说第一客户端节点 702 的任何有效应用程序会话。在一个实施例中，如果会话服务器 720 识别任何这样的有效应用程序会话，那么会话服务器 720 自动地将一个（或多个）应用程序会话与第一客户端节点 702 断开并且连接该一个（或多个）应用程序会话到当前客户端计算机 716。在一些实施例中，所接收的认证信息将限制客户端节点 702 重新连接到的应用程序会话。在一个实施例中，用户可以触发会话服务器的自动查阅以及随后与单个用户接口元件的选择的连接。

在识别与客户端节点 702 有关的应用程序会话之后，会话服务器 720 连接客户端节点 702 到相关的应用程序会话。会话服务器 720 确定所述多个应用程序会话中的每一个是有效还是断开的。在一个实施例中，所述多个应用程序会话中的至少一个是有效的。在一个实施例中，所述多个应用程序会话中的至少一个是断开的。在一个实施例中，会话服务器 720 自动接收应用程序输出。在另一实施例中，应用程序输出的接收由客户端节点 702 触发单个用户接口元件的选择。会话服务器 720 基于包含在所接收的信息 714 中的访问控制决定识别与客户端节点 702 重新连接的断开的的应用程序会话。在一个实施例中，一旦识别任何断开的的应用程序会话，则会话服务器 720 提示用户表示是否希望连接。如果不希望连接，则会话服务器 720 提示用户表示断开的的应用程序会话是否应当保持断开，或者应用程序会话是否应当终止。

在一个实施例中，连接包括修改所存储的应用程序数据库 722 中的项目以表示用户被连接到应用程序会话并且表示用户从那个客户端节点 702 连接到服务器。一旦连接，服务器 726 重新开始传送应用程序输出数据到客户端节点 702 或 716。在一个实施例中，与客户端节点有关的所述多个应用程序会话在连接之前被连接到第一客户端节点 702 并且，在连接之后所述多个应用程序会话被重新连接到第一客户端节点 702。在另一实施例中，与所述客户端节点有关的所述多个应用程序会话在连接之前被连接到第一客户端节点 702 并且，在连接之后所述多个应用程序会话被重新连接到第二客户端节点 716。

下面的示例性例子示出了上面讨论的方法和设备如何被用于提供

基于政策的对客户端节点的文件内容的访问。这些例子用于示例而不是用来限制本发明。

### 证据收集

在一个实施例中，客户端节点 102 请求访问位于政策机 106 所位于的同一网络的服务器上的文字处理文档。政策机 106 接收请求并且确定它不拥有任何关于客户端节点 102 的信息。政策机 106 传送收集代理 104 到客户端节点 102。在一些实施例中，收集代理 104 具有从客户端节点进行收集的预定义信息。在其它实施例中，收集代理 104 首先分析客户端节点来确定将要收集什么类型的信息。在又一个实施例中，收集代理 104 从政策机 106 取回关于将要收集关于客户端节点 102 的什么信息的指令。

一旦在客户端节点 102 上执行，则收集代理 104 收集所请求的信息并且传送该信息 112 给政策机 106。政策机 106 接收信息 112 并且开始确定信息 112 满足什么条件的处理。在一些实施例中，政策机 106 确定所接收的信息 112 不足够用于确定信息 112 是否满足一个或多个条件。在那些实施例中，政策机 106 传送另外的指令给收集代理 104 用于收集关于客户端节点 102 的更多信息。

### 基于政策的访问控制

当政策机 106 的第一部件 202 确定满足一个或多个条件时，它存储每个满足条件的标识符到数据组中。一旦完成，第一部件 202 传送该数据组以及所请求的应用程序给第二部件 210。在这个实施例的一个例子中，所请求的应用程序可以是文字处理文档并且所满足的条件可以表示客户端设备是个人数字助理。在这个实施例的另一个例子中，所请求的应用程序可以是电子制表软件并且所满足的条件可以表示客户端设备是从不安全网络比如公共互联网公用电话亭连接的受信任的膝上型计算机。在这个实施例的第三个例子中，所请求的应用程序可以是添加到电子邮件消息的文件并且所满足的条件可以表示客户端设备在从安全网络连接的但缺少适当的应用程序软件来观看该文件的个人桌上型计算机上。

第二部件 210 从第一部件 202 接收数据组并且应用一个或多个政

策到所接收的数据。在这个实施例的一个例子中，第二部件 210 可以应用政策，该政策要求当客户端设备类型为个人数字助理时如果客户端节点在其上具有应用程序软件的条件不满足，则客户端节点接收转换的文件内容。客户端节点将然后接收能够连接到转换服务器的可执行文件，转换服务器将以对于客户端设备类型可访问的格式呈现文件内容。应用这个政策使得客户端节点能够观看文件内容，而不管用于观看的不适当形式因素。

在这个实施例的又一个例子中，第二部件 210 可以应用政策，当客户端设备类型为受信任的膝上型计算机时该政策禁止下载到客户端节点 102，所述膝上型计算机包含适当的但来自不安全网络比如互联网公用电话亭的应用程序软件。在这个实施例中，政策可能要求政策机 106 传送可执行文件给客户端节点 102，客户端节点 102 使得能够连接到应用程序服务器 416 以用于呈现文件内容。应用这个类型的政策并且取回文件仅给应用程序服务器 416，使得客户端节点 102 能够观看文件内容而不危及来自不适当散布的私有文件内容。

在这个实施例的又一个例子中，第二部件 210 可以应用政策，该政策要求个人桌上型计算机做出安全连接，但缺乏适当的应用程序软件，通过 ICA 会话将个人桌上型计算机连接到应用程序服务器 416，并且要求应用程序服务器 416 执行适当的应用程序并且将该文件呈现给客户端节点 102。应用该政策使得客户端节点 102 能够观看文件内容而不管在客户端节点 102 上是否缺少应用程序软件。

本发明可以提供为包含在一项或多项产品上或在一项或多项产品中的一个或多个计算机可读程序。所述项产品可以是软盘、硬盘、光盘、数字多能光盘、高速存储器卡、PROM、RAM、ROM、或磁带。一般而言，计算机可读程序可以以任何编程语言来实现。可以使用的语言的一些例子包括 C、C++、C#、或 JAVA。软件程序可以被存储在一项或多项产品上或在一项或多项产品中作为目标代码。

虽然已经参照特定优选实施例加以示出和描述了本发明，但是本领域的技术人员应当理解，可以在形式和细节上对其做出各种变化而不背离下面权利要求所限定的本发明的宗旨和范围。

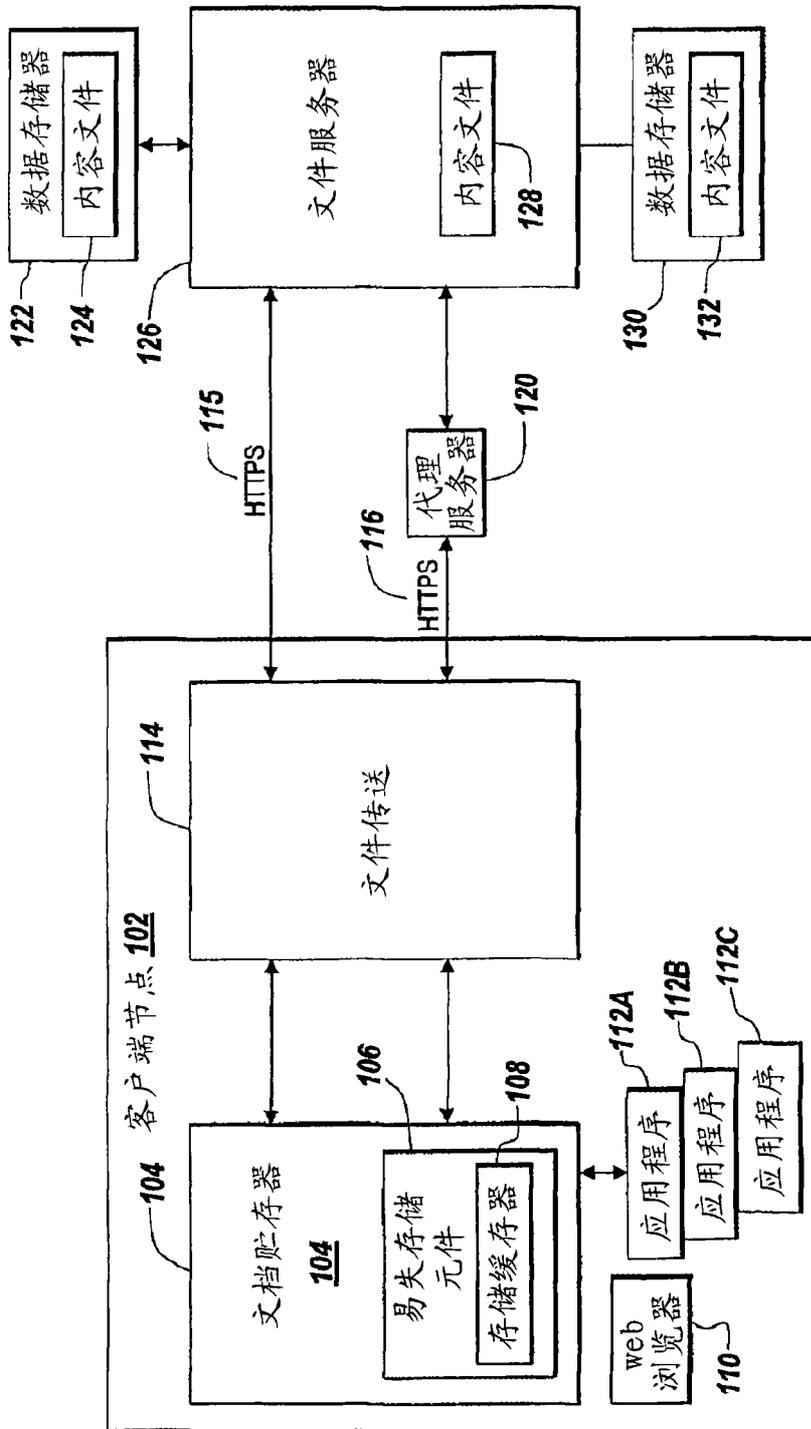


图 1A

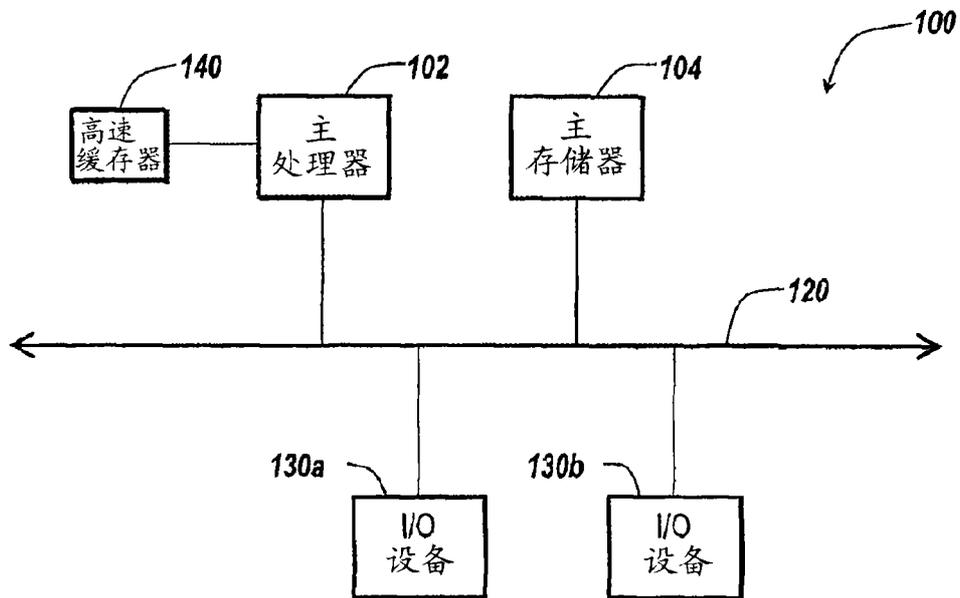


图 1B

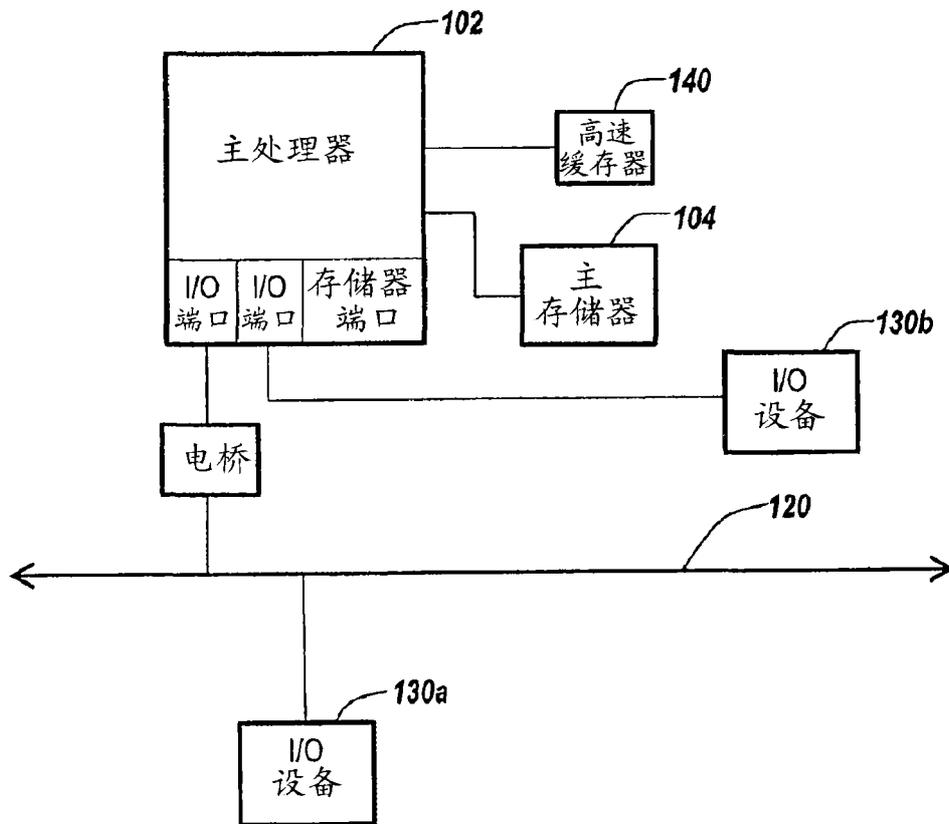


图 10

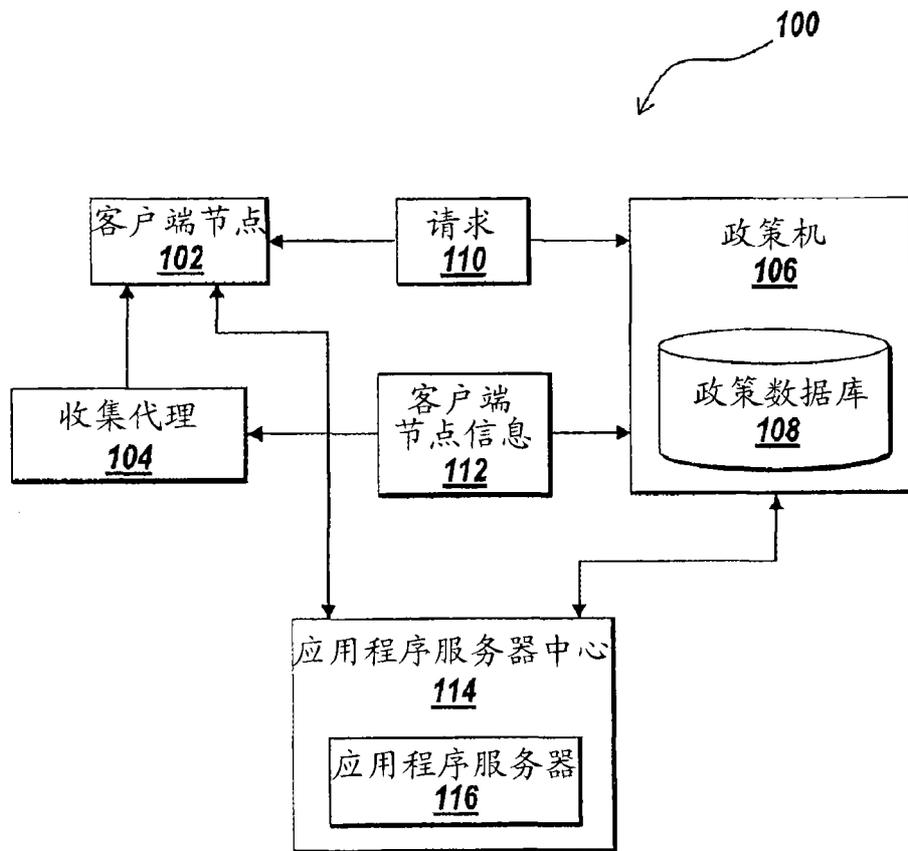


图 1D

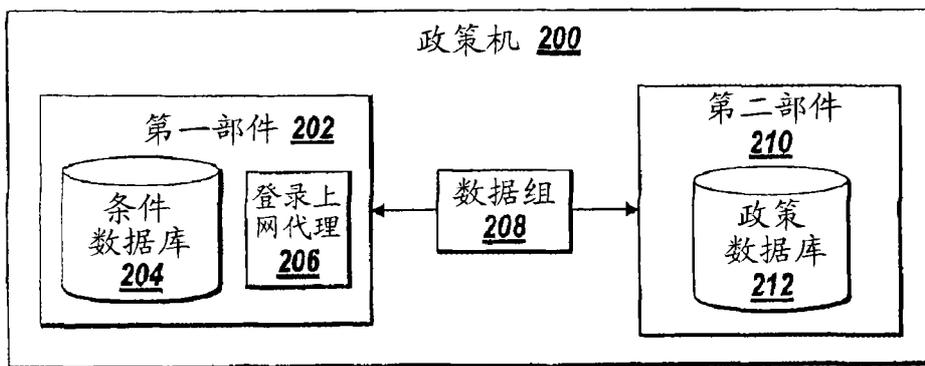


图 2

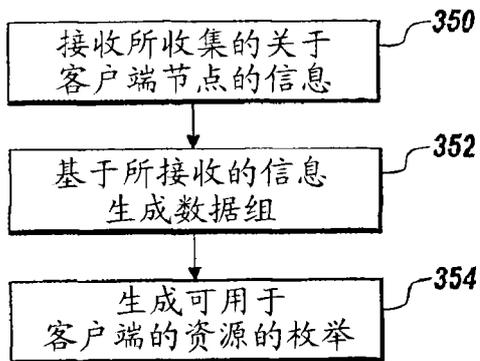


图 3

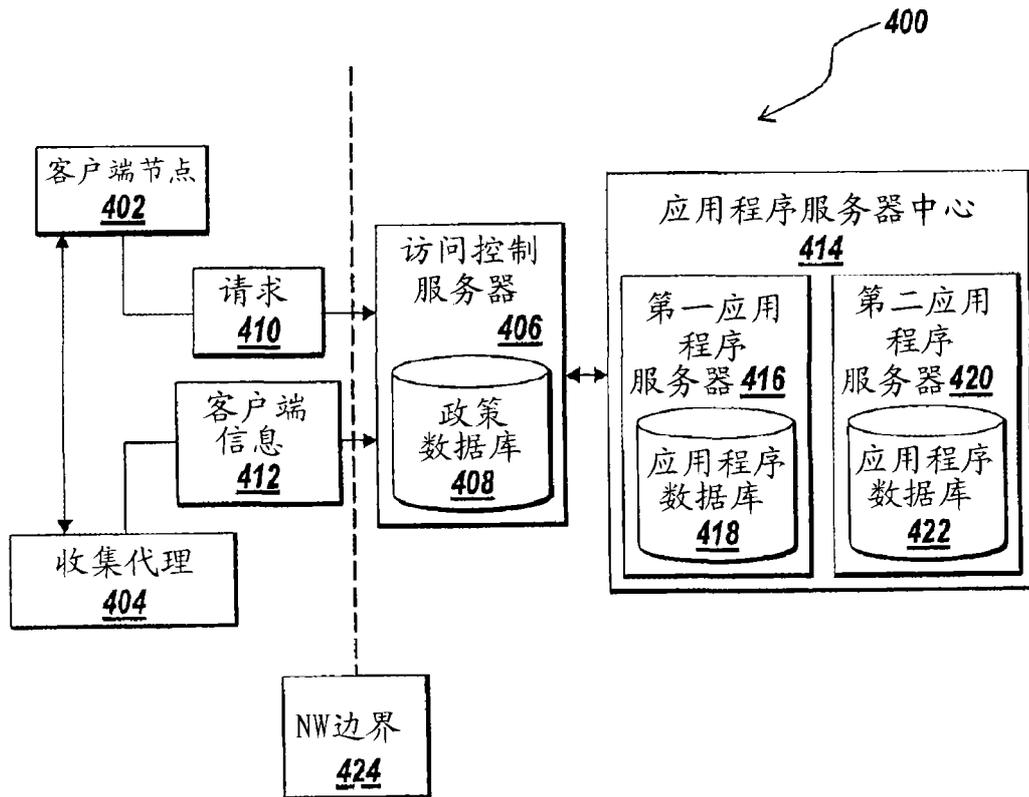


图 4

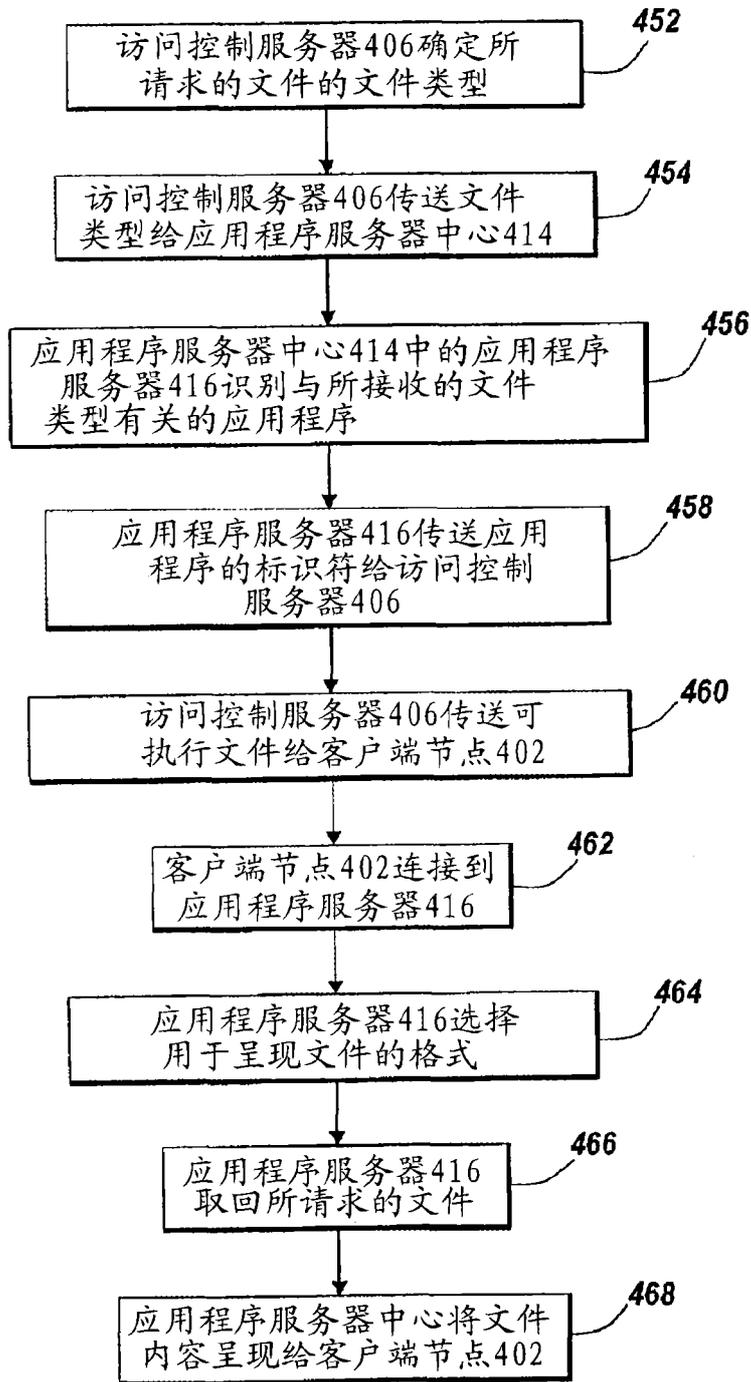


图 4B

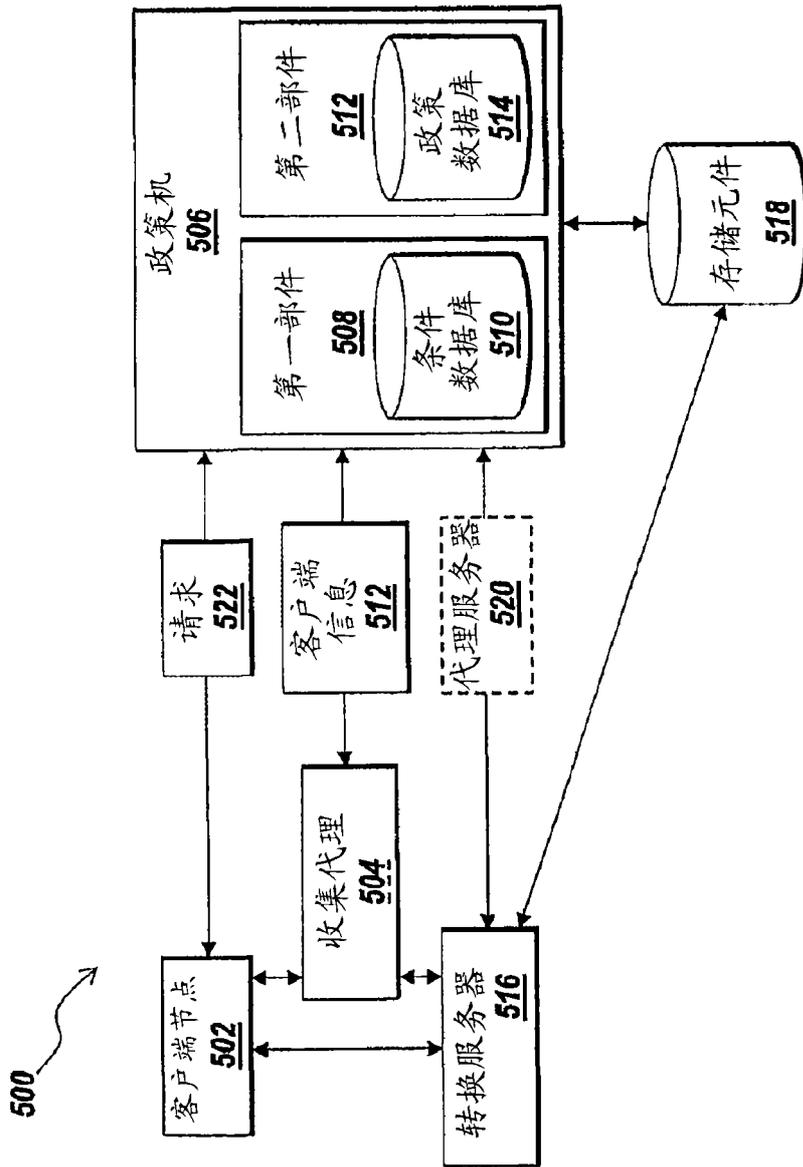


图 5

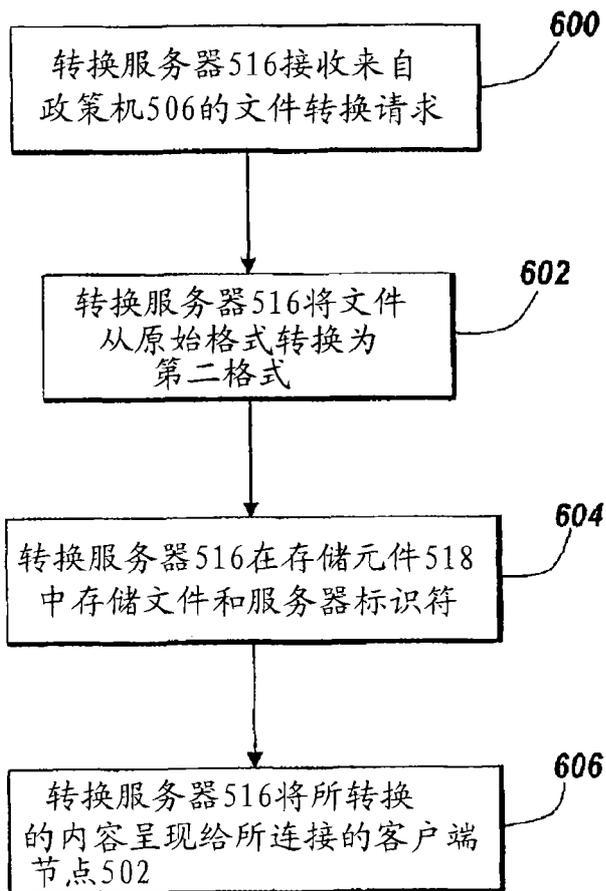


图 6

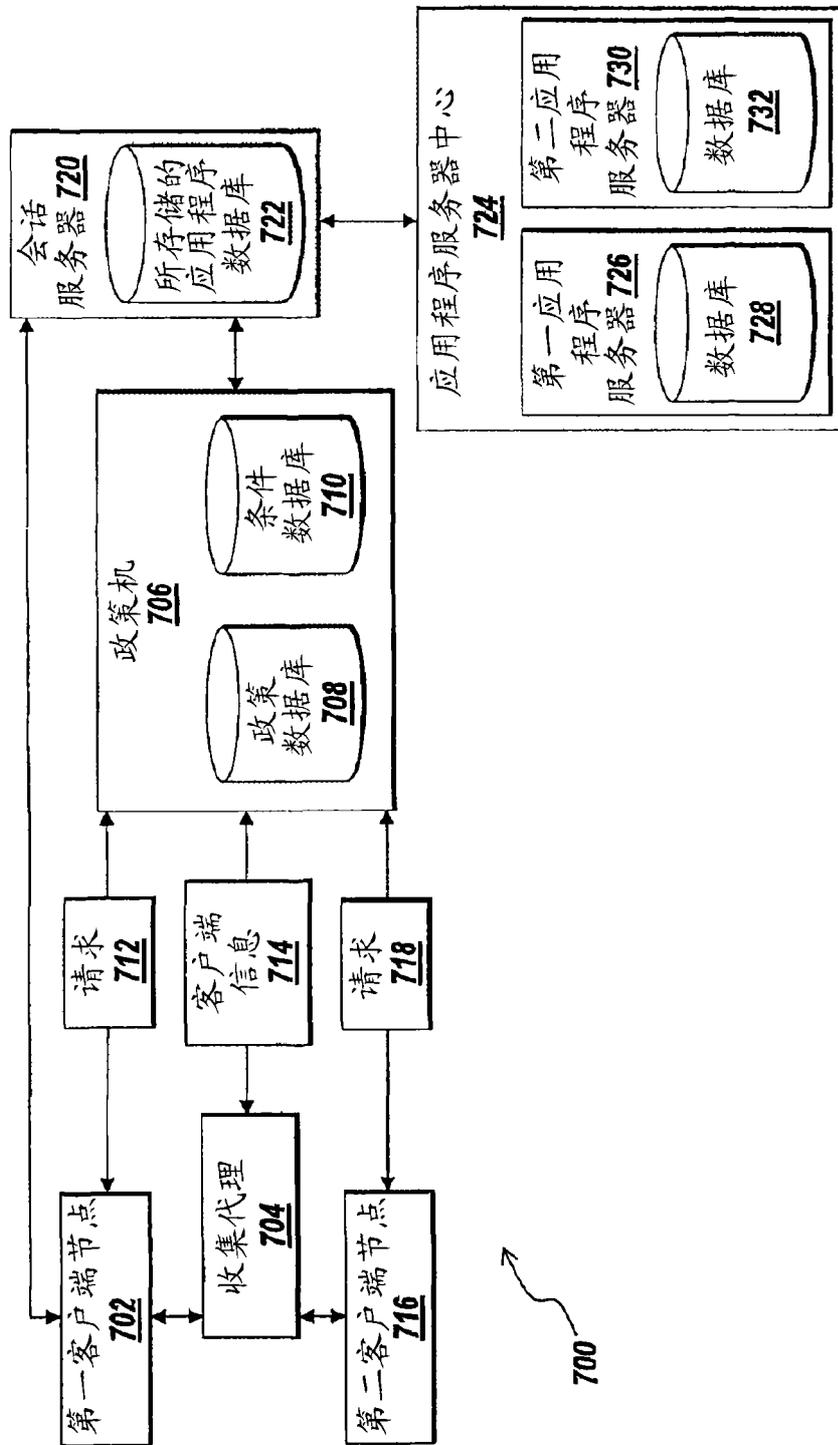


图 7

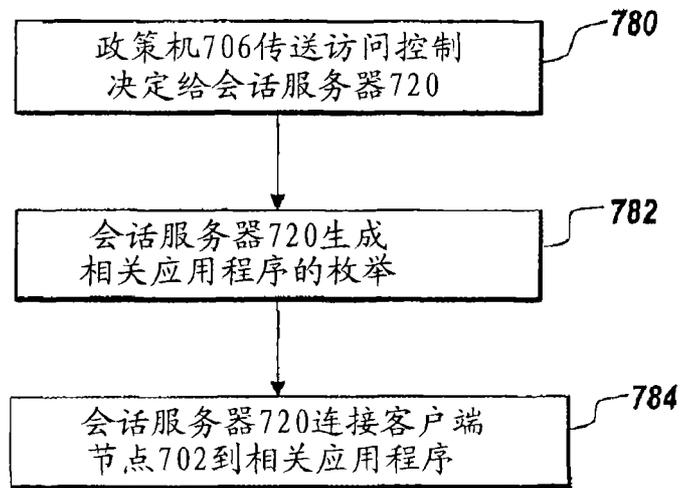


图 7B