



(12)发明专利

(10)授权公告号 CN 105359156 B

(45)授权公告日 2018.06.12

(21)申请号 201480038116.2

(74)专利代理机构 北京三友知识产权代理有限公司 11127

(22)申请日 2014.06.19

代理人 李辉 黄纶伟

(65)同一申请的已公布的文献号

申请公布号 CN 105359156 A

(51)Int.Cl.

G06F 21/55(2006.01)

(43)申请公布日 2016.02.24

G06F 21/31(2006.01)

(30)优先权数据

G06F 21/56(2006.01)

2013-141770 2013.07.05 JP

G06F 21/62(2006.01)

2013-141772 2013.07.05 JP

(56)对比文件

(85)PCT国际申请进入国家阶段日

WO 2009/032379 A1,2009.03.12,

2015.12.31

US 2009/0328216 A1,2009.12.31,

(86)PCT国际申请的申请数据

CN 102473221 A,2012.05.23,

PCT/JP2014/066272 2014.06.19

CN 103108074 A,2013.05.15,

(87)PCT国际申请的公布数据

CN 101960465 A,2011.01.26,

W02015/001969 JA 2015.01.08

CN 102315992 A,2012.01.11,

(73)专利权人 日本电信电话株式会社

Takeshi YAGI."design of an FTP

地址 日本东京都

honeypot for expanding the search scope

(72)发明人 秋山满昭 八木毅

in attack space",.《CSS2012 comouter

security symposium 2012 ronbunshu》.2012,

page 823-827..

审查员 于萍

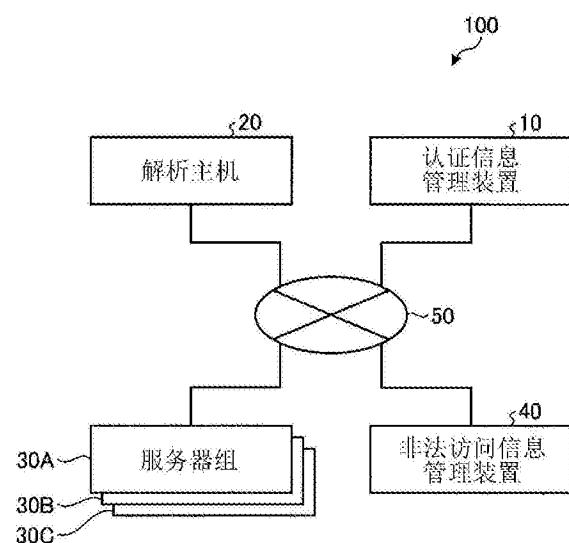
权利要求书2页 说明书18页 附图19页

(54)发明名称

非法访问检测系统和非法访问检测方法

(57)摘要

在非法访问检测系统(100)中生成向外部泄漏的认证信息。而且，在非法访问检测系统(100)中，将所生成的认证信息设定在解析主机(20)上，使解析对象程序在该解析主机(20)上进行动作。而且，在非法访问检测系统(100)中，对使用了认证信息的针对内容的访问进行检测，在检测出使用了认证信息的访问的情况下，将该访问确定为非法访问。



1. 一种非法访问检测系统,其特征在于,  
该非法访问检测系统具有:  
生成部,其生成认证信息;  
动作部,其将由所述生成部生成的认证信息设定在主机上,且使解析对象程序在该主机上进行动作;  
检测部,其对使用了所述认证信息的针对内容的非法访问进行检测;以及  
确定部,其在由所述检测部检测出使用了所述认证信息的非法访问的情况下,参照解析用认证信息存储部中存储的表,获取与所述非法访问中使用的认证信息对应的所述解析对象程序,且将所获取的在设定有该认证信息的主机上进行动作的所述解析对象程序确定为进行信息泄漏的程序,其中所述解析用认证信息存储部存储有规定了所述认证信息与设定了该认证信息的程序之间的对应关系的表。
2. 根据权利要求1所述的非法访问检测系统,其特征在于,  
该非法访问检测系统还具有存储部,所述存储部存储由所述生成部生成的认证信息,  
所述检测部判定所述针对内容的访问中使用的认证信息是否与所述存储部中存储的认证信息一致,在一致的情况下检测为非法访问。
3. 根据权利要求1或2所述的非法访问检测系统,其特征在于,  
该非法访问检测系统还具有删除部,在检测由所述确定部确定的程序而检测出了该程序的情况下,所述删除部删除该程序。
4. 根据权利要求1或2所述的非法访问检测系统,其特征在于,  
该非法访问检测系统还具有收集部,所述收集部从网络空间收集与由所述确定部确定的程序相同的程序。
5. 一种非法访问检测方法,由非法访问检测系统执行该非法访问检测方法,其特征在于,  
该非法访问检测方法包括:  
生成步骤,生成认证信息;  
动作步骤,在主机上设定通过所述生成步骤生成的认证信息,且使解析对象程序在该主机上进行动作;  
检测步骤,对使用了所述认证信息的针对内容的非法访问进行检测;以及  
确定步骤,在通过所述检测步骤检测出使用了所述认证信息的非法访问的情况下,参照解析用认证信息存储部中存储的表,获取与所述非法访问中使用的认证信息对应的所述解析对象程序,且将所获取的在设定有该认证信息的主机上进行动作的所述解析对象程序确定为进行信息泄漏的程序,其中所述解析用认证信息存储部存储有规定了所述认证信息与设定了该认证信息的程序之间的对应关系的表。
6. 根据权利要求5所述的非法访问检测方法,其特征在于,  
该非法访问检测方法还包括储存步骤,在所述储存步骤中,将通过所述生成步骤生成的认证信息储存于存储部中,  
在所述检测步骤中,判定所述针对内容的访问中使用的认证信息是否与所述存储部中存储的认证信息一致,在一致的情况下,检测为非法访问。
7. 根据权利要求5或6所述的非法访问检测方法,其特征在于,

该非法访问检测方法还包括删除步骤,在所述删除步骤中,在检测通过所述确定步骤确定的程序而检测出了该程序的情况下,删除该程序。

8.根据权利要求5或6所述的非法访问检测方法,其特征在于,  
该非法访问检测方法还包括收集步骤,在所述收集步骤中,从网络空间收集与通过所述确定步骤确定的程序相同的程序。

## 非法访问检测系统和非法访问检测方法

### 技术领域

[0001] 本发明涉及非法访问检测系统和非法访问检测方法。

### 背景技术

[0002] 近年来,计算机终端或服务器(在此,不对二者进行区分,以下记为主机)被作为具有恶意的软件的恶意软件(malware)感染,从而发生主机内部的信息被破坏或被恶意使用于以主机自身为跳板的新攻击中的事例。此外,恶意软件也可以未经允许而向外部泄漏主机内的信息。不仅是个人信息,还有可能泄漏公司、政府或者军事机关等的机密信息,因此恶意软件感染造成的信息泄漏成为问题。

[0003] 该恶意软件通过各种感染路径感染的方法已得到确认,例如为:通过伪装成邮件附件而导致用户误点击和安装而造成的感染;下载和安装伪装成在Web站点发布的一般的软件的恶意软件、伪装成P2P文件的恶意软件、在使用具有漏洞的Web浏览器浏览包含攻击代码的Web站点的情况下自动地下载和安装恶意软件而造成的感染等。

[0004] 此外,发生对在因特网上提供的各种服务的非法访问。大多数的非法访问存在如下两种情况:通过以蛮力方式(Brute Force)(攻击者以账户名和密码的所有可能的组合来尝试的登录)破解认证信息(例如,账户名和密码)来进行非法访问的情况;使用预先从用户那里通过某些方法盗取的正规的认证信息来进行非法访问的情况。在以蛮力方式破解认证信息的情况下,因为发生连续的登录的实施,因此能够基于单位时间的登录尝试次数的阈值利用IPS(Intrusion Prevention System:入侵防止系统)等进行检测和防御(例如,参照非专利文献1)。

[0005] 此外,针对这些恶意软件感染,防病毒销售商制作恶意软件的标志(signature),防止主机被恶意软件感染。但是,因为标志需要恶意软件的详细的解析,因此需要用于制作标志的时间成本。

[0006] 作为以往的信息泄漏对策,大多数对用户设定针对信息的访问权限,来防止机密数据的流出。此时,并没有将拥有访问权限的用户故意地向外部泄漏信息的情况作为对象。此外,当该用户复制了信息的情况下,并没有将针对复制后的数据的保护作为对象。

[0007] 另一方面,近年来,作为基于信息中心的控制的信息泄漏防止方法,使用了被称为DLP(Data Loss Prevention:数据丢失预防,或者,Data Leak Prevention:数据泄漏预防)的技术(例如,参照非专利文献2~4)。DLP对于具有机密性的信息,监视对该信息的访问和发送,特别防止向外部发送的情况。此时,有如下方法:在主机上进行信息控制的方法;以及在网络上通过监视通信内容来控制的方法。

[0008] 作为前者的在主机上进行信息控制的方法,公知有使用安装于用户所使用的主机上的代理程序来监视对机密信息的访问的方法。例如,在要从文件服务器下载机密信息而复制到USB存储器等外部存储设备的情况下,在画面上显示警告文等进行防御。在作为邮件的附件要向外部发送的情况下也通过同样的处理进行防御。

[0009] 作为后者的在网络上监视通信内容的方法,公知有使用对网络上的通信进行分析

的设备来在网络上监视通信内容的方法。例如,在作为邮件的附件要向外部发送机密信息的情况下,设备确认通信内容而进行阻止。

[0010] 现有技术文献

[0011] 非专利文献

[0012] 非专利文献1:“Suricata Downloads”、[online]、[平成25年5月15日检索]、因特网<<http://www.openinfosecfoundation.org/index.php/download-suricata>>

[0013] 非专利文献2:“Trend Micro Data Loss Prevention”、[online]、[平成25年5月1日检索]、因特网<<http://jp.trendmicro.com/jp/products/enterprise/tmdlp/>>

[0014] 非专利文献3:“RSA DLP (Data Loss Prevention) Suite”、[online]、[平成25年5月1日检索]、因特网<<http://japan.rsa.com/node.aspx?id=3426>>

[0015] 非专利文献4:“McAfee Data Loss Prevention Endpoint”、[online]、[平成25年5月1日检索]、因特网<[http://www.mcafee.com/japan/products/data\\_loss\\_prevention.asp](http://www.mcafee.com/japan/products/data_loss_prevention.asp)>

## 发明内容

[0016] 发明要解决的课题

[0017] 但是,在以往的技术中,存在如下课题:有时候无法恰当地确定非法访问、或者无法恰当地确定进行非法访问的程序。

[0018] 例如,在使用从用户那里通过某些方法盗取的正规的认证信息进行了非法访问的情况下,因为攻击者使用正确的认证信息进行登录,因此难以判别正规用户的访问和攻击者的访问。由此,恰当地进行使用了已泄漏的认证信息的非法访问的检测成为课题。

[0019] 此外,例如,使用上述的代理程序来在主机上进行信息控制的方法中,在被恶意软件感染的情况下,可以考虑到停止该代理程序之后再进行动作的情况。因此,在主机上难以完全地防御信息泄漏动作。

[0020] 此外,例如,上述的网络上监视通信内容的方法中,在恶意软件对通信内容进行了加密的情况下,仅靠通信内容难以确定实际上发送哪种种类的信息。

[0021] 此外,例如,虽然在因特网中存在多种多样的程序,但要判别这样的程序是否是进行信息泄漏的恶意软件,而需要程序的详细的解析。但是,因为在恶意软件中一般具有代码的加扰或反调试等抗解析功能,并且因为通信内容自身也多数被加密,因此难以确定是否进行信息泄漏。

[0022] 因此,本发明目的在于恰当地确定非法访问、或者恰当地确定进行非法访问的程序。

[0023] 用于解决课题的手段

[0024] 为了解决上述课题,实现目的,非法访问检测系统的特征在于,该非法访问检测系统具有:生成部,其生成向外部泄漏的认证信息;动作部,其将由所述生成部生成的认证信息设定在主机上,且使解析对象程序在该主机上进行动作;检测部,其对使用了所述认证信息的针对内容的访问进行检测;以及确定部,其在由所述检测部检测出使用了所述认证信息的访问的情况下,将该访问确定为非法访问。

[0025] 此外,非法访问检测方法是由非法访问检测系统执行的非法访问检测方法,其特

征在于，该非法访问检测方法包括：生成步骤，生成向外部泄漏的认证信息；动作步骤，将通过所述生成步骤生成的认证信息设定在主机上，且使解析对象程序在该主机上进行动作；检测步骤，对使用了所述认证信息的针对内容的访问进行检测；以及确定步骤，在通过所述检测步骤检测出使用了所述认证信息的访问的情况下，将该访问确定为非法访问。

[0026] 此外，非法访问检测系统的特征在于，该非法访问检测系统具有：生成部，其生成认证信息；动作部，其由所述生成部生成的认证信息设定在主机上，且使解析对象程序在该主机上进行动作；检测部，其对使用了所述认证信息的针对内容的非法访问进行检测；以及确定部，其在由所述检测部检测出使用了所述认证信息的非法访问的情况下，将在设定有该认证信息的主机上进行动作的程序确定为进行信息泄漏的程序。

[0027] 此外，非法访问检测方法是由非法访问检测系统执行的非法访问检测方法，其特征在于，该非法访问检测方法包括：生成步骤，生成认证信息；动作步骤，将通过所述生成步骤生成的认证信息设定在主机上，且使解析对象程序在该主机上进行动作；检测步骤，对使用了所述认证信息的针对内容的非法访问进行检测；以及确定步骤，在通过所述检测步骤检测出使用了所述认证信息的非法访问的情况下，将在设定有该认证信息的主机上进行动作的程序确定为进行信息泄漏的程序。

[0028] 发明效果

[0029] 本申请所公开的非法访问检测系统和非法访问检测方法能够恰当地确定非法访问、或者恰当地确定进行非法访问的程序。

## 附图说明

[0030] 图1是示出第一实施方式的非法访问检测系统的结构的一例的图。

[0031] 图2是说明第一实施方式的非法访问检测系统中解析用认证信息的泄漏处理、以及利用设定了解析用认证信息的服务来监视非法访问的处理的图。

[0032] 图3是示出第一实施方式的认证信息管理装置的结构的框图。

[0033] 图4是示出第一实施方式的解析主机的结构的框图。

[0034] 图5是示出第一实施方式的服务器的结构的框图。

[0035] 图6是说明第一实施方式的非法访问检测系统中使用了认证信息的信息泄漏检测处理的图。

[0036] 图7是示出第一实施方式的非法访问信息管理装置的结构的框图。

[0037] 图8是说明第一实施方式的非法访问检测系统中对进行非法访问的攻击者的主机进行过滤时的处理的图。

[0038] 图9是说明第一实施方式的非法访问检测系统中防止非法访问的处理的图。

[0039] 图10是用于说明第一实施方式的非法访问检测系统的服务器中的非法访问检测处理的流程的流程图。

[0040] 图11是示出第二实施方式的非法访问检测系统的结构的一例的图。

[0041] 图12是说明第二实施方式的非法访问检测系统中解析用认证信息的泄漏处理、以及利用设定了解析用认证信息的服务来监视非法访问的处理的图。

[0042] 图13是示出第二实施方式的认证信息管理装置的结构的框图。

[0043] 图14是示出解析用认证信息存储部中存储的表的一例的图。

- [0044] 图15是示出第二实施方式的解析主机的结构的框图。
- [0045] 图16是说明使用了单个和多个认证信息的解析处理的图。
- [0046] 图17是示出第二实施方式的服务器的结构的框图。
- [0047] 图18是说明第二实施方式的非法访问检测系统中使用了认证信息的信息泄漏检测处理的图。
- [0048] 图19是说明第二实施方式的非法访问检测系统中进行信息泄漏的恶意软件的确定处理的图。
- [0049] 图20是用于说明第二实施方式的非法访问检测系统的服务器中的非法访问检测处理的流程的流程图。
- [0050] 图21是示出执行非法访问检测程序的计算机的图。

## 具体实施方式

[0051] 以下参照附图详细地说明本发明的非法访问检测系统和非法访问检测方法的实施方式。另外，本发明不限于该实施方式。

### [第一实施方式]

[0053] 在以下的实施方式中，按顺序说明第一实施方式的非法访问检测系统和非法访问检测方法的处理的流程，最后说明第一实施方式的效果。

### [系统的结构]

[0055] 首先，说明第一实施方式的非法访问检测系统100的结构的一例。图1是示出第一实施方式的非法访问检测系统的结构的一例的图。如图1所示，非法访问检测系统100具有认证信息管理装置10、解析主机20和服务器组30A～30C、以及非法访问信息管理装置40。此外，在非法访问检测系统100中，认证信息管理装置10、解析主机20、以及服务器组30A～30C经由因特网50而分别连接。另外，对于服务器组30A～30C，当不进行特别区分而对一台服务器进行说明的情况下，记载为服务器30。

[0056] 认证信息管理装置10生成解析用的认证信息，且管理所生成的认证信息与设定认证信息的程序之间的对应关系。此外，认证信息管理装置10向解析主机20进行发送。此时，所生成的认证信息与各服务器30A～30C对应，作为认证信息而生成服务的站点信息、账户名以及密码。服务的站点信息是提供用于对使用解析用的认证信息的非法访问进行监视的服务的服务器的信息，例如是服务器组30A～30C的IP地址或者FQDN。此外，账户名和密码随机生成，生成实际上未被使用的内容。

[0057] 解析主机20将某个特定服务的认证信息设定在解析主机20上，且使解析对象程序进行动作。此时，解析主机20与因特网50连接。在程序是进行信息泄漏的恶意软件的情况下，未经用户的同意偷偷地向外部的攻击者泄漏认证信息。

[0058] 服务器组30A～30C是管理Web站点的内容的服务器，是用于使攻击者以故意泄漏给攻击者的认证信息进行非法访问的服务器。例如，当发生了利用已泄漏的认证信息进行的访问的情况下，服务器组30A～30C确定该访问是非法访问，且获取进行了该非法访问的攻击者的主机信息(例如，IP地址)而向非法访问信息管理装置40发送。

[0059] 非法访问信息管理装置40管理进行了非法访问的攻击者的主机信息，且对服务器组30A～30C发送主机信息。由此，对于服务器组30A～30C来说，在各种服务中以进行了非法

访问的攻击者的主机作为过滤对象。

[0060] 在非法访问检测系统100中,作为前提,敢于泄漏解析用的认证信息来监视非法访问的处理。在此,使用图2来说明解析用认证信息的泄漏处理、以及利用设定了解析用认证信息的服务来监视非法访问的处理。图2是说明第一实施方式的非法访问检测系统中解析用认证信息的泄漏处理、以及利用设定了解析用认证信息的服务来监视非法访问的处理的图。

[0061] 如图2所示,首先,解析主机20将由认证信息管理装置10生成的认证信息作为某个特定服务的认证信息设定在解析主机上,当使程序动作时,在进行解析的程序是进行信息泄漏的恶意软件的情况下,访问储存有前述的认证信息的文件、注册表(参照图2的(1))。而且,解析主机20未经用户的同意偷偷地向外部的攻击者泄漏认证信息(参照图2的(2))。

[0062] 接着,使提供某个特定服务的服务器组30A~30C进行动作,且观测登录。此时,在攻击者进行了使用被泄漏的认证信息的登录的情况下(参照图2的(3)),服务器组30A~30C判断该访问是非法访问(参照图2的(4))。

[0063] 这样,通过敢于泄漏解析用的认证信息,在使用了与被泄漏的认证信息相同的认证信息的时候,能够确定该访问是非法访问。而且,获取进行了非法访问的攻击者的主机信息,且在各种服务中过滤该主机信息,从而能够检测非法访问且防患于未然。

[0064] [认证信息管理装置的结构]

[0065] 接着,说明图3所示的认证信息管理装置10的结构。图3是示出第一实施方式的认证信息管理装置的结构的框图。如图3所示,认证信息管理装置10具有通信处理部11、控制部12以及存储部13。

[0066] 通信处理部11对在与所连接的解析主机20、服务器组30A~30C等之间进行交换的各种信息所涉及的通信进行控制。例如,通信处理部11对解析主机20发送所生成的认证信息。此外,例如,通信处理部11从服务器组30A~30C接收用于非法访问的认证信息。

[0067] 如图3所示,存储部13具有解析用认证信息存储部13a。存储部13例如是RAM(Random Access Memory:随机存取存储器)、闪存(Flash Memory)等半导体存储元件,或者是硬盘、光盘等存储装置等。

[0068] 解析用认证信息存储部13a存储表,该表规定了由后述的生成部12a生成的解析用的认证信息、与设定了该认证信息的程序之间的对应关系。

[0069] 在此,例如,解析用认证信息存储部13a存储服务的站点信息、账户名、密码等作为用于解析的认证信息。服务的站点信息例如是与提供用于对使用解析用的认证信息的非法访问进行监视的服务的服务器组30A~30C相关的信息,例如是IP地址或者FQDN(Fully Qualified Domain Name:完全限定域名)。

[0070] 此外,解析用认证信息存储部13a例如存储未在实际的服务中使用的账户名作为账户名。此外,解析用认证信息存储部13a存储难以推测的充分复杂的字符串作为密码。这是为了当在登录时识别是否是泄漏信息时,与基于蛮力方式的登录攻击进行识别。

[0071] 返回图3,控制部12具有生成部12a和管理部12b。在此,控制部12是CPU(Central Processing Unit:中央处理器)或MPU(Micro Processing Unit:微处理器)等电子电路、或者ASIC(Application Specific Integrated Circuit:专用集成电路)或FPGA(Field Programmable Gate Array:现场可编程门阵列)等集成电路。

[0072] 生成部12a生成向外部泄漏的认证信息。例如,生成部12a生成服务器组30A～30C的IP地址或者FQDN、与随机生成的账户名和密码的组合,作为敢于泄漏给攻击者的解析用的认证信息。另外,所生成的认证信息只要与各种种类的服务对应即可,例如是SSH(Secure Shell:安全外壳)、FTP(File Transfer Protocol:文件传输协议)、POP(Post Office Protocol:邮局协议)等。

[0073] 另外,为了在提供服务的服务器30中准确地区分针对该服务的蛮力方式的登录(攻击者以账户名和密码的所有可能的组合来尝试的登录)、和使用了已泄漏的认证信息的登录,所生成的解析用认证信息优选是随机生成的充分长的唯一的字符串。

[0074] 管理部12b向解析主机20发送由生成部12a生成的认证信息。在此所发送的认证信息被设定于解析主机20上,且执行解析对象的程序。此外,管理部12b接收与解析主机20所执行的程序对应的认证信息的组,且将程序和与程序对应的认证信息的组对应起来储存于解析用认证信息存储部13a中。

[0075] [解析主机的结构]

[0076] 接着,说明图4所示的解析主机20的结构。图4是示出第一实施方式的解析主机的结构的框图。如图4所示,解析主机20具有通信处理部21、控制部22以及存储部23。

[0077] 通信处理部21对在与所连接的认证信息管理装置10、服务器组30A～30C等之间进行交换的各种信息所涉及的通信进行控制。例如,通信处理部21从认证信息管理装置10接收认证信息。此外,例如,通信处理部21向外部的攻击者发送认证信息。另外,在从认证信息管理装置10接收了认证信息的情况下,将所接收的认证信息储存于后述的解析用认证信息存储部23a中。

[0078] 如图4所示,存储部23具有解析用认证信息存储部23a。存储部23例如是RAM(Random Access Memory:随机存取存储器)、闪存(Flash Memory)等半导体存储元件,或者是硬盘、光盘等存储装置等。

[0079] 解析用认证信息存储部23a存储由前述的认证信息管理装置10生成的解析用的认证信息。例如,解析用认证信息存储部23a存储服务的站点信息、账户名、密码等作为用于解析的认证信息。服务的站点信息例如是与提供用于对使用解析用的认证信息的非法访问进行监视的服务的服务器组30A～30C相关的信息,例如是IP地址或者FQDN(Fully Qualified Domain Name:完全限定域名)。

[0080] 此外,解析用认证信息存储部23a例如存储未在实际的服务中使用的账户名作为账户名。此外,解析用认证信息存储部23a存储难以推测的充分复杂的字符串作为密码。这是为了当在登录时识别是否是泄漏信息时,与基于蛮力方式的登录攻击进行识别。

[0081] 返回图4,控制部22具有设定部22a和动作部22b。在此,控制部22是CPU(Central Processing Unit:中央处理器)或MPU(Micro Processing Unit:微处理器)等电子电路、或者ASIC(Application Specific Integrated Circuit:专用集成电路)或FPGA(Field Programmable Gate Array:现场可编程门阵列)等集成电路。

[0082] 设定部22a将由认证信息管理装置10的生成部12a生成的认证信息设定为特定服务的认证信息。例如,设定部22a从解析用认证信息存储部23a获取认证信息,且将所获取的认证信息设定为特定服务的认证信息。

[0083] 动作部22b使服务的客户端应用程序(SSH、FTP、POP等)作为解析对象程序而在由

设定部22a设定了认证信息的解析主机20上进行动作。而且,动作部22b通知与所执行的程序对应的认证信息的组。在此,在进行动作的程序是进行信息泄漏的恶意软件的情况下,未经用户的同意偷偷地向外部的攻击者泄漏认证信息。被泄漏的认证信息可以是任何种类的服务,只要在提供服务的服务器30侧能够确认是否存在被泄漏的认证信息的登录即可。此外,关于服务,既可以准备成用于解析,也可以使用实际的服务。

[0084] [服务器的结构]

[0085] 接着,说明图5所示的服务器30的结构。图5是示出第一实施方式的服务器的结构的框图。如图5所示,服务器30具有通信处理部31、控制部32以及存储部33。

[0086] 通信处理部31对在与所连接的认证信息管理装置10、解析主机20等之间进行交换的各种信息所涉及的通信进行控制。例如,通信处理部31对认证信息管理装置10发送用于非法访问的认证信息。此外,通信处理部31从认证信息管理装置10接收解析用认证信息。在此所接收的解析用认证信息被存储于解析用认证信息存储部33a中。

[0087] 如图5所示,存储部33具有解析用认证信息存储部33a和非法主机信息存储部33b。存储部33例如是RAM (Random Access Memory:随机存取存储器)、闪存(Flash Memory)等半导体存储元件,或者是硬盘、光盘等存储装置等。

[0088] 解析用认证信息存储部33a存储由前述的认证信息管理装置10生成的解析用的认证信息的列表。为了由后述的检测部32a判定登录是否是非法访问,而使用解析用认证信息存储部33a中存储的认证信息的列表。

[0089] 例如,解析用认证信息存储部33a存储服务的站点信息、账户名、密码等作为用于解析的认证信息。服务的站点信息例如是与提供用于对使用解析用的认证信息的非法访问进行监视的服务的服务器30相关的信息,例如是IP地址或者FQDN (Fully Qualified Domain Name:完全限定域名)。

[0090] 此外,解析用认证信息存储部33a例如存储未在实际的服务中使用的账户名作为账户名。此外,解析用认证信息存储部33a存储难以推测的充分复杂的字符串作为密码。这是为了当在登录时识别是否是泄漏信息时,与基于蛮力方式的登录攻击进行识别。

[0091] 非法主机信息存储部33b存储进行了非法访问的主机的信息。例如,非法主机信息存储部33b存储IP地址作为进行了非法访问的主机的信息。

[0092] 返回图5,控制部32具有检测部32a、确定部32b、储存部32c以及访问防止部32d。在此,控制部32是CPU (Central Processing Unit:中央处理器) 或MPU (Micro Processing Unit:微处理器) 等电子电路、或者ASIC (Application Specific Integrated Circuit:专用集成电路) 或FPGA (Field Programmable Gate Array:现场可编程门阵列) 等集成电路。

[0093] 检测部32a对使用了由认证信息管理装置10的生成部12a生成的认证信息的针对内容的访问进行检测。具体而言,检测部32a判定针对内容的访问中使用的认证信息是否与解析用认证信息存储部33a中存储的认证信息一致。

[0094] 在由检测部32a检测出使用了认证信息的访问的情况下,确定部32b将该访问确定为非法访问。例如,在针对准备了与解析用认证信息对应的解析用账户的内容发生了登录事件的情况下,确定部32b判定用于该登录的认证信息是否被包含于解析用认证信息存储部33a中存储的解析用认证信息中。

[0095] 其结果为,在用于登录的认证信息被包含于解析用认证信息存储部33a中存储的

解析用认证信息的列表的情况下,确定部32b将登录确定为非法访问,且对认证信息管理装置10发送用于非法访问的认证信息。

[0096] 储存部32c获取进行了由确定部32b确定为非法访问的访问的主机的信息而储存于非法主机信息存储部33b中。此外,储存部32c向非法访问信息管理装置40发送所获取的主机的信息。

[0097] 访问防止部32d检测来自根据非法主机信息存储部33b中存储的主机信息而确定的主机的访问,防止来自该主机的访问。例如,访问防止部32d判定尝试登录的主机是否被包含于攻击者主机信息中,且在判定的结果为被包含的情况下,判断为是攻击者的登录,且拦截登录。

[0098] 在此,使用图6说明第一实施方式的非法访问检测系统100中使用了认证信息的信息泄漏检测处理。图6是说明第一实施方式的非法访问检测系统中使用了认证信息的信息泄漏检测处理的图。如图6所示,非法访问检测系统100的认证信息管理装置10,每当进行程序的解析时,每次生成唯一的解析用认证信息(提供服务的服务器名、账户名以及密码信息的组)(参照图6的(1))。

[0099] 而且,将所生成的解析用认证信息设定于执行程序的解析主机20上(参照图6的(2)),且执行解析对象的程序(参照图6的(3))。此外,解析主机20向认证信息管理装置10通知与所执行的程序对应的认证信息的组(参照图6的(4))。而且,认证信息管理装置10针对提供服务的服务器30通知所生成的解析用认证信息(参照图6的(5))。

[0100] 之后,解析主机20在执行了解析对象的程序之后,在该程序是进行信息泄漏的恶意软件的情况下向攻击者发送所设定的解析用认证信息(参照图6的(6))。此时,不需要对程序是否进行了信息泄漏进行识别。攻击者使用已泄漏的认证信息,对该服务进行非法访问,来尝试登录(参照图6的(7))。提供该服务的服务器30对登录是否是使用了解析用认证信息的登录进行识别,在是使用了解析用认证信息的登录的情况下,检测为是非法访问(参照图6的(8))。此时获取进行了非法访问的主机的信息且进行存储,由此,在各种服务中将该主机的信息作为过滤对象。

[0101] [非法访问信息管理装置的结构]

[0102] 接着,说明图7所示的非法访问信息管理装置40的结构。图7是示出第一实施方式的非法访问信息管理装置的结构的框图。如图7所示,非法访问信息管理装置40具有通信处理部41、控制部42以及存储部43。

[0103] 通信处理部41对在与所连接的认证信息管理装置10、解析主机20、服务器30等之间进行交换的各种信息所涉及的通信进行控制。例如,通信处理部41从服务器30接收进行了非法访问的主机的信息。此外,通信处理部41向服务器组30A~30C发送进行了非法访问的主机的信息。

[0104] 如图7所示,存储部43具有非法主机信息存储部43a和服务器信息存储部43b。存储部43例如是RAM(Random Access Memory:随机存取存储器)、闪存(Flash Memory)等半导体存储元件,或者是硬盘、光盘等存储装置等。

[0105] 非法主机信息存储部43a存储进行了非法访问的主机信息的列表(以下有时记载为攻击者主机信息列表)。例如,非法主机信息存储部43a存储IP地址作为进行了非法访问的主机信息的列表。在此被存储的信息是从服务器组30A~30C收集的主机信息的列表。

[0106] 服务器信息存储部43b存储对进行了非法访问的主机的信息进行通知的服务器的地址信息等。在此被存储的信息在后述的发送部42b向服务器30发送进行了非法访问的主机的信息时被参照。

[0107] 返回图7,控制部42具有储存部42a和发送部42b。在此,控制部42是CPU(Central Processing Unit:中央处理器)或MPU(Micro Processing Unit:微处理器)等电子电路、或者ASIC(Application Specific Integrated Circuit:专用集成电路)或FPGA(Field Programmable Gate Array:现场可编程门阵列)等集成电路。

[0108] 储存部42a接收从服务器30发送的进行了非法访问的主机的信息,且将进行了非法访问的主机的信息储存于非法主机信息存储部43a中。例如,储存部42a将IP地址作为进行了非法访问的主机的信息而储存于非法主机信息存储部43a中,来更新攻击者主机信息列表。

[0109] 当使用解析用认证信息判别为在某个服务中是非法访问时能够收集的攻击者主机信息列表,能够应用于实际的使用各种认证信息的服务中。若是公司内部系统或使用用户被限定的服务,则通过限定主机的IP地址等,能够在某种程度上防御因账户信息泄漏而导致的非法访问。例如,若是公司内部系统,则能够通过设为仅从公司内部的IP地址登录来进行防御。但是,因为进行登录的主机庞大地存在,并且IP地址也分散,因此,不确定的多数的用户使用的服务无法采用通过预先制限使用者的IP地址的对策。在本实施方式中,也可以应用于后者的不确定的多数使用的服务中,作为例子能够举出例如邮件服务、因特网购物服务、社交网络服务、博客(blog)服务等。

[0110] 发送部42b向各服务器30A~30C发送进行了非法访问的主机的信息。例如,发送部42b参照服务器信息存储部43b中存储的服务器30的地址信息,向各服务器30A~30C发送进行了非法访问的主机的信息。

[0111] 使用图8说明对进行非法访问的攻击者的主机进行过滤时的处理。图8是说明第一实施方式的非法访问检测系统中对进行非法访问的攻击者的主机进行过滤时的处理的图。如图8所示,提供服务的服务器30A检测出使用了解析用认证信息的非法访问的情况下(参照图8的(1)),向非法访问信息管理装置40发送该攻击者的主机信息(参照图8的(2))。

[0112] 而且,非法访问信息管理装置40发送对其他服务器(服务器30B、服务器30C)发送进行非法访问的攻击者的主机信息(参照图8的(3))。接收了攻击者的信息的各服务器30A~30C,当受到非法访问时(参照图8的(4)),基于该信息而与登录时的主机信息进行比较,从而识别攻击者的主机,防止非法访问(参照图8的(5))。另外,提供服务的服务器30既可以存在多个种类,也可以是单一服务器。

[0113] 在此,使用图9说明第一实施方式的非法访问检测系统100中防止非法访问的处理。图9是说明第一实施方式的非法访问检测系统中防止非法访问的处理的图。

[0114] 如图9所示,解析主机20将由认证信息管理装置10生成的认证信息作为某个特定服务的认证信息设定在解析主机20上,当使程序动作时,在进行解析的程序是进行信息泄漏的恶意软件的情况下,访问储存有前述的认证信息的文件、注册表(参照图9的(1))。而且,解析主机20未经用户的同意偷偷地向外部的攻击者泄漏认证信息(参照图9的(2))。

[0115] 接着,使提供某个特定服务的服务器30进行动作,且观测登录。此时,在攻击者进行了使用被泄漏的认证信息的登录的情况下(参照图9的(3)),服务器30将该登录判断为是

非法访问(参照图9的(4))。而且,通过在其他服务的访问过滤中有效利用进行了非法访问的主机信息而能够防止非法访问。

[0116] [服务器的处理]

[0117] 接着,使用图10说明第一实施方式的服务器30的处理。图10是用于说明第一实施方式的非法访问检测系统的服务器中的非法访问检测处理的流程图。

[0118] 如图10所示,服务器30的通信处理部31判定是否从认证信息管理装置10接收了解析用认证信息(步骤S101)。其结果为,通信处理部31在未从认证信息管理装置10接收解析用认证信息的情况下(步骤S101否定),进入步骤S103的处理。此外,通信处理部31在从认证信息管理装置10接收了解析用认证信息的情况下(步骤S101肯定),更新解析用认证信息存储部33a中存储的比较用的解析用认证信息的列表(步骤S102)。

[0119] 而且,储存部32c判定是否从非法访问信息管理装置40接收了攻击者的主机信息(步骤S103)。其结果为,储存部32c在未从非法访问信息管理装置40接收攻击者的主机信息的情况下(步骤S103否定),进入步骤S105的处理。此外,储存部32c在从非法访问信息管理装置40接收了攻击者的主机信息的情况下(步骤S103肯定),通过将主机信息储存于非法主机信息存储部33b中,来更新比较用的攻击者主机信息列表(步骤S104)。

[0120] 而且,检测部32a针对准备了与解析用认证信息对应的解析用账户的内容,判定是否发生了登录事件(步骤S105)。其结果为,在没有发生登录事件的情况下(步骤S105否定),返回到步骤S101的处理。此外,在发生了登录事件的情况下(步骤S105肯定),检测部32a判定用于该登录的认证信息是否被包含于解析用认证信息存储部33a中存储的解析用认证信息中(步骤S106)。

[0121] 其结果为,在用于登录的认证信息被包含于解析用认证信息存储部33a中存储的解析用认证信息中的情况下(步骤S106肯定),确定部32b将登录判定为非法访问(步骤S107)。接着,确定部32b向认证信息管理装置10通知用于非法访问的认证信息(步骤S108),进入步骤S112的处理。

[0122] 此外,在步骤S106中,在用于登录的认证信息未被包含于解析用认证信息存储部33a中存储的解析用认证信息中的情况下(步骤S106否定),访问防止部32d判定尝试登录的主机是否被包含于攻击者主机信息中(步骤S109)。其结果为,访问防止部32d在判定为尝试登录的主机未被包含于攻击者主机信息中的情况下(步骤S109否定),将登录判定为正常访问(步骤S110),进入步骤S112的处理。此外,访问防止部32d在判定为尝试登录的主机被包含于攻击者主机信息中的情况下(步骤S109肯定),判断为是攻击者的登录,且拦截登录(步骤S111),进入步骤S112的处理。

[0123] 在步骤S112中,检测部32a判定是否继续进行非法访问的监视(步骤S112)。其结果为,检测部32a在判定为继续进行非法访问的监视的情况下(步骤S112肯定),返回到步骤S101。此外,检测部32a在判定为不继续进行非法访问的监视的情况下(步骤S112否定),结束处理。

[0124] [第一实施方式的效果]

[0125] 如上述那样,在第一实施方式的非法访问检测系统100中,生成向外部泄漏的认证信息,且在主机上设定所生成的认证信息,使解析对象程序在该主机上进行动作。而且,在非法访问检测系统100中,对使用了认证信息的针对内容的访问进行检测,在检测出使用了

认证信息的访问的情况下,将该访问确定为非法访问。因此,能够恰当地进行使用了已泄漏的认证信息的非法访问的检测和防御。

[0126] 此外,在攻击者使用通过信息泄漏所获取的认证信息对各种服务进行了非法访问的情况下,在入侵检测系统中难以判别正规的用户和攻击者,但在非法访问检测系统100中,因为被泄漏的信息自身是用于解析的,而一般用户不会使用,因此在该信息被使用的时候能够判别为是非法访问,并且能够确定进行了该非法访问的攻击者的主机。该攻击者的主机在其他各种服务中进行非法访问的可能性也高,因此,通过在其他各种服务中过滤该主机信息(例如IP地址)而能够检测非法访问且防患于未然。

[0127] [第二实施方式]

[0128] 虽然在上述的第一实施方式中,对检测使用了已泄漏的认证信息的非法访问的情况进行了说明,但本实施方式并不限于此。例如,也可以确定进行信息泄漏的恶意软件。因此,以下,作为第二实施方式,说明如下情况的例子:非法访问检测系统在对使用了认证信息的针对内容的非法访问进行检测而检测出使用了认证信息的非法访问的情况下,将在设定有该认证信息的主机上进行动作的程序确定为进行信息泄漏的程序。

[0129] [系统的结构]

[0130] 首先,说明第二实施方式的非法访问检测系统200的结构的一例。图11是示出第二实施方式的非法访问检测系统的结构的一例的图。如图11所示,非法访问检测系统200具有认证信息管理装置210、解析主机220以及服务器组230A~230C。此外,在非法访问检测系统200中,认证信息管理装置210、解析主机220、以及服务器组230A~230C经由因特网240而分别连接。另外,对于服务器组230A~230C,当不进行特别区分而对一台服务器进行说明的情况下,记载为服务器230。

[0131] 认证信息管理装置210生成解析用的认证信息,且管理所生成的认证信息与设定认证信息的程序之间的对应关系。此外,认证信息管理装置210向解析主机220进行发送。此时,所生成的认证信息是与各服务器230A~230C对应的,作为认证信息而生成服务的站点信息、账户名以及密码。服务的站点信息是提供用于对使用解析用的认证信息的非法访问进行监视的服务的服务器的信息,例如是服务器组230A~230C的IP地址或者FQDN。此外,账户名和密码随机生成,生成实际上未被使用的内容。

[0132] 此外,认证信息管理装置210在从服务器组230A~230C接收了用于非法访问的认证信息的情况下,将与所接收的认证信息对应的程序确定为进行信息泄漏的程序。

[0133] 解析主机220将某个特定服务的认证信息设定在解析主机220上,且使解析对象程序进行动作。此时,解析主机220与因特网240连接。在程序是进行信息泄漏的恶意软件的情况下,未经用户的同意偷偷地向外部的攻击者泄漏认证信息。

[0134] 服务器组230A~230C是管理Web站点的内容的服务器,是用于使攻击者以故意泄漏给攻击者的认证信息进行非法访问的服务器。例如,当发生了利用已泄漏的认证信息进行的访问的情况下,服务器组230A~230C确定该访问是非法访问,且向认证信息管理装置210通知被利用的认证信息。

[0135] 在非法访问检测系统200中,作为前提,进行敢于泄漏解析用的认证信息、且监视非法访问的处理。在此,使用图12说明解析用认证信息的泄漏处理、以及利用设定了解析用认证信息的服务来监视非法访问的处理。图12是说明第二实施方式的非法访问检测系统中

解析用认证信息的泄漏处理、以及利用设定了解析用认证信息的服务来监视非法访问的处理的图。

[0136] 如图12所示,首先,解析主机220将由认证信息管理装置210生成的认证信息作为某个特定服务的认证信息设定在解析主机上,当使程序动作时,在进行解析的程序是进行信息泄漏的恶意软件的情况下,访问储存有前述的认证信息的文件、注册表(参照图12的(1))。而且,解析主机220未经用户的同意偷偷地向外部的攻击者泄漏认证信息(参照图12的(2))。

[0137] 接着,使提供某个特定服务的服务器组230A~230C进行动作,且观测登录。此时,在攻击者进行了使用被泄漏的认证信息的登录的情况下(参照图12的(3)),服务器组230A~230C判断该访问是非法访问(参照图12的(4))。

[0138] 这样,通过敢于泄漏解析用的认证信息,在使用了与被泄漏的认证信息相同的认证信息的时候,能够确定该访问是非法访问。而且,将与用于非法访问的认证信息对应的程序确定为进行信息泄漏的程序。

[0139] [认证信息管理装置的结构]

[0140] 接着,说明图13所示的认证信息管理装置210的结构。图13是示出第二实施方式的认证信息管理装置的结构的框图。如图13所示,认证信息管理装置210具有通信处理部211、控制部212以及存储部213。

[0141] 通信处理部211对在与所连接的解析主机220、服务器组230A~230C等之间进行交换的各种信息所涉及的通信进行控制。例如,通信处理部211对解析主机220发送所生成的认证信息。此外,例如,通信处理部211从服务器组230A~230C接收用于非法访问的认证信息。

[0142] 如图13所示,存储部213具有解析用认证信息存储部213a和恶性程序存储部213b。存储部213例如是RAM(Random Access Memory:随机存取存储器)、闪存(Flash Memory)等半导体存储元件,或者是硬盘、光盘等存储装置等。

[0143] 解析用认证信息存储部213a存储表,该表规定了由后述的生成部212a生成的解析用的认证信息、与设定了该认证信息的程序之间的对应关系。例如,如图14所例示的那样,解析用认证信息存储部213a将作为对解析对象的程序进行识别的信息的“解析程序”、表示在解析主机220上进行动作的应用程序的种类的“客户端应用程序”、作为对所生成的认证信息进行识别的信息的“认证信息”对应起来存储。

[0144] 在此,例如,解析用认证信息存储部213a存储服务的站点信息、账户名、密码等作为用于解析的认证信息。服务的站点信息例如是与提供用于对使用解析用的认证信息的非法访问进行监视的服务的服务器组230A~230C相关的信息,例如是IP地址或者FQDN(Fully Qualified Domain Name:完全限定域名)。

[0145] 此外,解析用认证信息存储部213a例如存储未在实际的服务中使用的账户名作为账户名。此外,解析用认证信息存储部213a存储难以推测的充分复杂的字符串作为密码。这是为了当在登录时识别是否是泄漏信息时,与基于蛮力方式的登录攻击进行识别。

[0146] 恶性程序存储部213b存储对泄漏信息的恶性程序进行识别的信息。具体而言,恶性程序存储部213b存储对由后述的确定部212c确定的恶性程序进行识别的信息。

[0147] 返回图13,控制部212具有生成部212a、管理部212b、确定部212c、以及收集部

212d。在此,控制部212是CPU(Central Processing Unit:中央处理器)或MPU(Micro Processing Unit:微处理器)等电子电路、或者ASIC(Application Specific Integrated Circuit:专用集成电路)或FPGA(Field Programmable Gate Array:现场可编程门阵列)等集成电路。

[0148] 生成部212a生成向外部泄漏的认证信息。例如,生成部212a生成服务器组230A~230C的IP地址或者FQDN、与随机生成的账户名和密码的组合,作为敢于泄漏给攻击者的解析用的认证信息。另外,所生成的认证信息只要与各种种类的服务对应即可,例如是SSH(Secure Shell:安全外壳)、FTP(File Transfer Protocol:文件传输协议)、POP(Post Office Protocol:邮局协议)等。

[0149] 另外,为了在提供服务的服务器230中准确地区分针对该服务的蛮力方式的登录(攻击者以账户名和密码的所有可能的组合来尝试的登录)、和使用了已泄漏的认证信息的登录,所生成的解析用认证信息优选是随机生成的充分长的唯一的字符串。

[0150] 管理部212b向解析主机220发送由生成部212a生成的认证信息。在此发送的认证信息被设定于解析主机220上,且执行解析对象的程序。此外,管理部212b接收与解析主机220所执行的程序对应的认证信息的组,且将程序和与程序对应的认证信息的组对应起来储存于解析用认证信息存储部213a中。

[0151] 确定部212c在由后述的服务器230的检测部232a检测出使用了认证信息的非法访问的情况下,将在设定有该认证信息的解析主机220上进行动作的程序确定为进行信息泄漏的程序。例如,确定部212c当从服务器组230A~230C接收到在非法访问中使用的认证信息时,参照解析用认证信息存储部233a中存储的表,获取与该认证信息对应的程序,且将该程序确定为进行信息泄漏的程序。

[0152] 收集部212d从网络空间(web space)收集与由确定部212c确定的程序相同的程序。例如,收集部212d也可以使用作为现有技术的Web客户端蜜罐技术通过巡回网络空间来进行收集。Web客户端蜜罐技术不仅能够收集通过攻击Web浏览器的漏洞来自动地下载和安装的程序,即使是通过弹出等而需要用户点击对话框来进行下载和安装的程序,也能够通过模拟用户交互来进行收集。特别是在这样的需要进行需要用户点击对话框的程序下载和安装的情况下,因为正规的程序和具有恶意的程序并存,因此能够基于是否进行信息泄漏来判别是否是恶意软件。

[0153] [解析主机的结构]

[0154] 接着,说明图15所示的解析主机220的结构。图15是示出第二实施方式的解析主机的结构的框图。如图15所示,解析主机220具有通信处理部221、控制部222以及存储部223。

[0155] 通信处理部221对在与所连接的认证信息管理装置210、服务器组230A~230C等之间进行交换的各种信息所涉及的通信进行控制。例如,通信处理部221从认证信息管理装置210接收认证信息。此外,例如,通信处理部221向外部的攻击者发送认证信息。另外,在从认证信息管理装置210接收了认证信息的情况下,将所接收的认证信息储存于后述的解析用认证信息存储部223a中。

[0156] 如图15所示,存储部223具有解析用认证信息存储部223a。存储部223例如是RAM(Random Access Memory:随机存取存储器)、闪存(Flash Memory)等半导体存储元件,或者是硬盘、光盘等存储装置等。

[0157] 解析用认证信息存储部223a存储由前述的认证信息管理装置210生成的解析用的认证信息。例如,解析用认证信息存储部223a存储服务的站点信息、账户名、密码等作为用于解析的认证信息。服务的站点信息例如是与提供用于对使用解析用的认证信息的非法访问进行监视的服务的服务器组230A~230C相关的信息,例如是IP地址或者FQDN(Fully Qualified Domain Name:完全限定域名)。

[0158] 此外,解析用认证信息存储部223a作为账户名例如存储未在实际的服务中使用的账户名。此外,解析用认证信息存储部223a存储难以推测的充分复杂的字符串作为密码。这是为了当在登录时识别是否是泄漏信息时,与基于蛮力方式的登录攻击进行识别。

[0159] 返回图15,控制部222具有设定部222a和动作部222b。在此,控制部222是CPU(Central Processing Unit:中央处理器)或MPU(Micro Processing Unit:微处理器)等电子电路、或者ASIC(Application Specific Integrated Circuit:专用集成电路)或FPGA(Field Programmable Gate Array:现场可编程门阵列)等集成电路。

[0160] 设定部222a将由认证信息管理装置210的生成部212a生成的认证信息设定为特定服务的认证信息。例如,设定部222a从解析用认证信息存储部223a获取认证信息,且将所获取的认证信息设定为特定服务的认证信息。

[0161] 动作部222b在由设定部222a设定了认证信息的解析主机220上使服务的客户端应用程序(SSH、FTP、POP等)作为解析对象程序进行动作。而且,动作部222b通知与所执行的程序对应的认证信息的组。在此,在进行动作的程序是进行信息泄漏的恶意软件的情况下,未经用户的同意偷偷地向外部的攻击者泄漏认证信息。被泄漏的认证信息可以是任何种类的服务,只要在提供服务的服务器230侧能够确认是否存在被泄漏的认证信息的登录即可。此外,关于服务,既可以准备成用于解析,也可以使用实际的服务。

[0162] 此外,在服务的客户端应用程序在解析主机220上进行动作的情况下,假定这些客户端应用程序将认证信息写入文件、注册表中。关于该设定用文件或注册表,由各客户端应用程序储存的路径和形式被预先确定,因此,基于此将认证信息写入文件、注册表中。

[0163] 在进行解析的程序是进行信息泄漏的恶意软件的情况下,访问储存有前述的认证信息的文件、注册表,且向外部发送该信息。对于认证信息的设定,既可以按每台主机设定在单一的特定客户端应用程序的文件、注册表中,也可以同时设定在多个客户端应用程序的文件、注册表中。另外,在同时将解析信息设定中多个客户端应用程序中的情况下,需要以所设定的客户端应用程序的种类来生成解析用认证信息。

[0164] 例如,如图16所例示的那样,作为将认证信息设定在单一的特定客户端应用程序的文件、注册表中的例子,解析主机220将“解析用认证信息A”设定在“SSH客户端应用程序的设定文件”中而使“程序1”进行动作。或者,不同的解析主机220将“解析用认证信息B”设定在“FTP客户端应用程序的设定文件”中而使“程序2”进行动作。

[0165] 此外,如图16所例示的那样,作为同时将解析用认证信息设定在多个客户端应用程序的文件、注册表中的例子,解析主机220将“解析用认证信息C”设定在“SSH客户端应用程序的设定文件”、且将“解析用认证信息D”设定在“FTP客户端应用程序的设定文件”、且将“解析用认证信息E”设定在“POP客户端应用程序的设定注册表”中而使“程序3”进行动作。

[0166] [服务器的结构]

[0167] 接着,说明图17所示的服务器230的结构。图17是示出第二实施方式的服务器的结

构的框图。如图17所示，服务器230具有通信处理部231、控制部232以及存储部233。

[0168] 通信处理部231对在与所连接的认证信息管理装置210、解析主机220等之间进行交换的各种信息所涉及的通信进行控制。例如，通信处理部231对认证信息管理装置210发送用于非法访问的认证信息。此外，通信处理部231从认证信息管理装置210接收解析用认证信息。在此所接收的解析用认证信息被存储于解析用认证信息存储部233a中。

[0169] 如图17所示，存储部233具有解析用认证信息存储部233a。存储部233例如是RAM (Random Access Memory:随机存取存储器)、闪存 (Flash Memory) 等半导体存储元件，或者是硬盘、光盘等存储装置等。

[0170] 解析用认证信息存储部233a存储由前述的认证信息管理装置210生成的解析用的认证信息的列表。为了由后述的检测部232a判定登录是否是非法访问，而使用解析用认证信息存储部233a中存储的认证信息的列表。

[0171] 例如，解析用认证信息存储部233a存储服务的站点信息、账户名、密码等作为用于解析的认证信息。服务的站点信息例如是与提供用于对使用解析用的认证信息的非法访问进行监视的服务的服务器230相关的信息，例如是IP地址或者FQDN (Fully Qualified Domain Name:完全限定域名)。

[0172] 此外，解析用认证信息存储部233a例如存储未在实际的服务中使用的账户名作为账户名。此外，解析用认证信息存储部233a存储难以推测的充分复杂的字符串作为密码。这是为了当在登录时识别是否是泄漏信息时，与基于蛮力方式的登录攻击进行识别。

[0173] 返回图17，控制部232具有检测部232a和删除部232b。在此，控制部232是CPU (Central Processing Unit:中央处理器) 或MPU (Micro Processing Unit:微处理器) 等电子电路、或者ASIC (Application Specific Integrated Circuit:专用集成电路) 或FPGA (Field Programmable Gate Array:现场可编程门阵列) 等集成电路。

[0174] 检测部232a对使用了由认证信息管理装置210的生成部212a生成的认证信息的针对内容的非法访问进行检测。具体而言，检测部232a判定针对内容的访问中使用的认证信息是否与解析用认证信息存储部233a中存储的认证信息一致，且在一致的情况下检测为非法访问。

[0175] 例如，在针对准备了与解析用认证信息对应的解析用账户的内容发生了登录事件的情况下，检测部232a判定用于该登录的认证信息是否被包含于解析用认证信息存储部233a中存储的解析用认证信息中。

[0176] 其结果为，在用于登录的认证信息被包含于解析用认证信息存储部233a中存储的解析用认证信息的列表中的情况下，检测部232a将登录判定为非法访问，且对认证信息管理装置210发送用于非法访问的认证信息。此外，在用于登录的认证信息未被包含于解析用认证信息存储部233a中存储的解析用认证信息的列表中的情况下，检测部232a将登录判定为正常访问。

[0177] 删除部232b在检测由认证信息管理装置210的确定部212c确定的程序且检测出了该程序的情况下，删除该程序。此外，例如，删除部232b在从认证信息管理装置210接收到对进行信息泄漏的程序进行识别的信息时，作为防止实际的主机受到进行信息泄漏的程序所导致的信息泄漏的损害的方法，能够禁止该程序在主机上的执行。登记该程序作为基于主机的入侵检测系统或防病毒软件的文件标志，在主机上存在文件的情况下或者在想要执行

它的情况下,进行禁止和删除。

[0178] 此外,作为防止实际的主机受到信息泄漏的损害的方法,能够禁止从网络下载该程序。利用基于网络的入侵检测系统、Web代理服务器、邮件服务器等进行监视,检查从外部网络下载的文件,在包含该程序的情况下禁止下载。

[0179] 在此,使用图18,说明第二实施方式的非法访问检测系统200中使用了认证信息的信息泄漏检测处理。图18是说明第二实施方式的非法访问检测系统中使用了认证信息的信息泄漏检测处理的图。如图18所示,非法访问检测系统200的认证信息管理装置210,每当进行程序的解析时,每次生成唯一的解析用认证信息(提供服务的服务器名、账户名以及密码信息的组)进行通知(参照图18的(1))。

[0180] 而且,将所生成的解析用认证信息设定于执行程序的解析主机220上(参照图18的(2)),且执行解析对象的程序(参照图18的(3))。此外,解析用主机220向认证信息管理装置210通知与所执行的程序对应的认证信息的组(参照图18的(4))。而且,认证信息管理装置210对提供服务的服务器230通知所生成的解析用认证信息(参照图18的(5))。

[0181] 之后,解析主机220在执行了解析对象的程序之后,在该程序是进行信息泄漏的恶意软件的情况下向攻击者发送所设定的解析用认证信息(参照图18的(6))。此时,不需要对程序是否进行了信息泄漏进行识别。攻击者使用已泄漏的认证信息,对该服务进行非法访问,来尝试登录(参照图18的(7))。提供该服务的服务器230对登录是否是使用了解析用认证信息的登录进行识别,在是使用了解析用认证信息的登录的情况下,检测为是非法访问(参照图18的(8))。因为能够根据此时使用的解析用认证信息来确定进行了解析的程序,因此得知该程序是进行信息泄漏的程序。

[0182] 在此,使用图19说明第二实施方式的非法访问检测系统200中进行信息泄漏的恶意软件的确定处理。图19是说明第二实施方式的非法访问检测系统中进行信息泄漏的恶意软件的确定处理的图。

[0183] 如图19所示,解析主机220将由认证信息管理装置210生成的认证信息作为某个特定服务的认证信息设定在解析主机220上,当使程序动作时,在进行解析的程序是进行信息泄漏的恶意软件的情况下,访问储存有前述的认证信息的文件、注册表(参照图19的(1))。而且,解析主机220未经用户的同意偷偷地向外部的攻击者泄漏认证信息(参照图19的(2))。

[0184] 接着,使提供某个特定服务的服务器230进行动作,且观测登录。此时,在攻击者进行了使用被泄漏的认证信息的登录的情况下(参照图19的(3)),服务器230将该登录判断为是非法访问(参照图19的(4))。而且,能够根据用于非法访问的认证信息来对设定该认证信息进行了解析的程序进行确定,还能够断定该程序进行了信息泄漏。因此,能够准确地确定进行信息泄漏的恶意软件。

[0185] [服务器的处理]

[0186] 接着,使用图20说明第二实施方式的服务器230的处理。图20是用于说明第二实施方式的非法访问检测系统的服务器中的非法访问检测处理的流程的流程图。

[0187] 如图20所示,服务器230的通信处理部231判定是否从认证信息管理装置210接收了解析用认证信息(步骤S201)。其结果为,通信处理部231在未从认证信息管理装置210接收解析用认证信息的情况下(步骤S201否定),进入步骤S203的处理。此外,通信处理部231

在从认证信息管理装置210接收了解析用认证信息的情况下(步骤S201肯定),更新解析用认证信息存储部233a中存储的比较用的解析用认证信息的列表(步骤S202)。

[0188] 而且,检测部232a针对准备了与解析用认证信息对应的解析用账户的内容,判定是否发生了登录事件(步骤S203)。其结果为,在没有发生登录事件的情况下(步骤S203否定),返回到步骤S201的处理。此外,在发生了登录事件的情况下(步骤S203肯定),检测部232a判定用于该登录的认证信息是否被包含于解析用认证信息存储部233a中存储的解析用认证信息中(步骤S204)。

[0189] 其结果为,在用于登录的认证信息未被包含于解析用认证信息存储部233a中存储的解析用认证信息中的情况下(步骤S204否定),检测部232a将登录判定为正常访问(步骤S206),进行后述的步骤S208的处理。此外,在用于登录的认证信息包含于解析用认证信息存储部233a中存储的解析用认证信息中的情况下(步骤S204肯定),检测部232a将登录判定为非法访问(步骤S205)。

[0190] 接着,检测部232a向认证信息管理装置210通知用于非法访问的认证信息(步骤S207),且判定是否继续进行非法访问的监视(步骤S208)。其结果为,检测部232a在判定为继续进行非法访问的监视的情况下(步骤S208肯定),返回到步骤S201。此外,检测部232a在判定为不继续进行非法访问的监视的情况下(步骤S208否定),结束处理。

[0191] [第二实施方式的效果]

[0192] 如上述那样,在第二实施方式的非法访问检测系统200中,生成认证信息,且在解析主机220上设定所生成的认证信息,使解析对象程序在该解析主机220上进行动作。而且,在对使用了认证信息的针对内容的非法访问进行检测而检测出使用了认证信息的非法访问的情况下,将在设定有该认证信息的解析主机220上进行动作的程序确定为进行信息泄漏的程序。因此,能够准确地确定进行信息泄漏的恶意软件。

[0193] 此外,在非法访问检测系统200中,程序、特别是恶意软件具有抗解析功能,程序代码的解析或行为的解析、通信内容的解析一般较为困难。在本实施方式中,在不对进行信息泄漏的代码的确定、程序的行为、或者程序向外部发送的通信内容进行解析的情况下,能够准确地确定进行信息泄漏的程序(恶意软件)。

[0194] [系统结构等]

[0195] 此外,图示的各装置的各结构要素是功能概念性的,在物理上未必需要如图示那样构成。即,各装置的分散/整合的具体方式并不限于图示的内容,能够根据各种负荷或使用状况等使其全部或者一部分以任意的单位在功能上或者物理上进行分散/整合而构成。例如,也可以对生成部12a和管理部12b进行整合。而且,在各装置所进行的各处理功能其全部或者任意的一部分可以通过CPU和由该CPU解析执行的程序来实现,或者能够作为基于布线逻辑的硬件来实现。

[0196] 此外,在本实施方式所说明的各处理中,能够手动执行作为自动执行的处理来说明的处理的全部或者一部分,或者也能够通过公知的方法自动执行作为手动执行的处理来说明的处理的全部或者一部分。此外,对于包含上述文档中或附图中所示出的处理步骤、控制步骤、具体的名称以及各种数据或参数在内的信息,除了特殊说明的情况之外能够任意地变更。

[0197] [程序]

[0198] 此外,也能够制作出一种程序,该程序利用计算机可执行的语言来描述了上述实施方式中说明的非法访问检测系统100、200中的各装置执行的处理。例如,也能够制作出一种非法访问检测程序,该非法访问检测程序利用计算机可执行的语言来描述了第一实施方式的非法访问检测系统100或者第二实施方式的非法访问检测系统200中的各装置执行的处理。在这种情况下,通过计算机执行非法访问检测程序,也能够获得与上述实施方式相同的效果。而且,也可以将该非法访问检测程序存储到计算机可读取的存储介质中,通过使计算机读入并执行该存储介质中存储的非法访问检测程序,来实现与上述第一实施方式或者第二实施方式相同的处理。

[0199] 图21是示出执行非法访问检测程序的计算机1000的图。如图21所例示的那样,计算机1000例如具有存储器1010、CPU 1020、硬盘驱动器接口1030、磁盘驱动器接口1040、串行端口接口1050、视频适配器1060以及网络接口1070,这些各部分由总线1080连接。

[0200] 如图21所例示的那样,存储器1010包含ROM (Read Only Memory: 只读存储器) 1011和RAM 1012。ROM 1011例如存储BIOS (Basic Input Output System: 基本输入输出系统) 等引导程序。如图21所例示的那样,硬盘驱动器接口1030与硬盘驱动器1031连接。如图21所例示的那样,磁盘驱动器接口1040与磁盘驱动器1041连接。例如磁盘或光盘等可装卸的存储介质插入到磁盘驱动器1041中。如图21所例示的那样,串行端口接口1050例如与鼠标1051、键盘1052连接。如图21所例示的那样,视频适配器1060例如与显示器1061连接。

[0201] 在此,如图21所例示的那样,硬盘驱动器1031例如存储OS 1091、应用程序1092、程序模块1093以及程序数据1094。即,上述的非法访问检测程序作为描述有由计算机1000执行的指令的程序模块而被存储于例如硬盘驱动器1031中。

[0202] 此外,在上述实施方式中说明的各种数据作为程序数据而被存储于例如存储器1010或硬盘驱动器1031中。而且,CPU 1020根据需要将存储器1010或硬盘驱动器1031中存储的程序模块1093或者程序数据1094读取到RAM 1012,且执行各种处理步骤。

[0203] 另外,与非法访问检测程序相关的程序模块1093或程序数据1094并不限于被存储于硬盘驱动器1031中的情况,例如也可以被存储于可装卸的存储介质中而经由磁盘驱动器等被CPU 1020所读取。或者,与非法访问检测程序相关的程序模块1093或程序数据1094也可以被存储于经由网络 (LAN (Local Area Network: 局域网)、WAN (Wide Area Network: 广域网) 等) 连接的其他计算机中,并经由网络接口1070被CPU 1020所读取。

[0204] 标号说明

[0205] 10、210:认证信息管理装置;11、21、31、41、211、221、231:通信处理部;12、22、32、42、212、222、232:控制部;12a、212a:生成部;12b、212b:管理部;13、23、33、43、213、223、233:存储部;13a、23a、33a、213a、223a、233a:解析用认证信息存储部;20、220:解析主机;22a、222a:设定部;22b、222b:动作部;30、230:服务器;32a、232a:检测部;32b:确定部;32c、42a:储存部;32d:访问防止部;33b、43a:非法主机信息存储部;40:非法访问信息管理装置;42b:发送部;43b:服务器信息存储部;50、240:因特网;100、200:非法访问检测系统;212c:确定部;212d:收集部;213b:恶性程序存储部;232b:删除部。

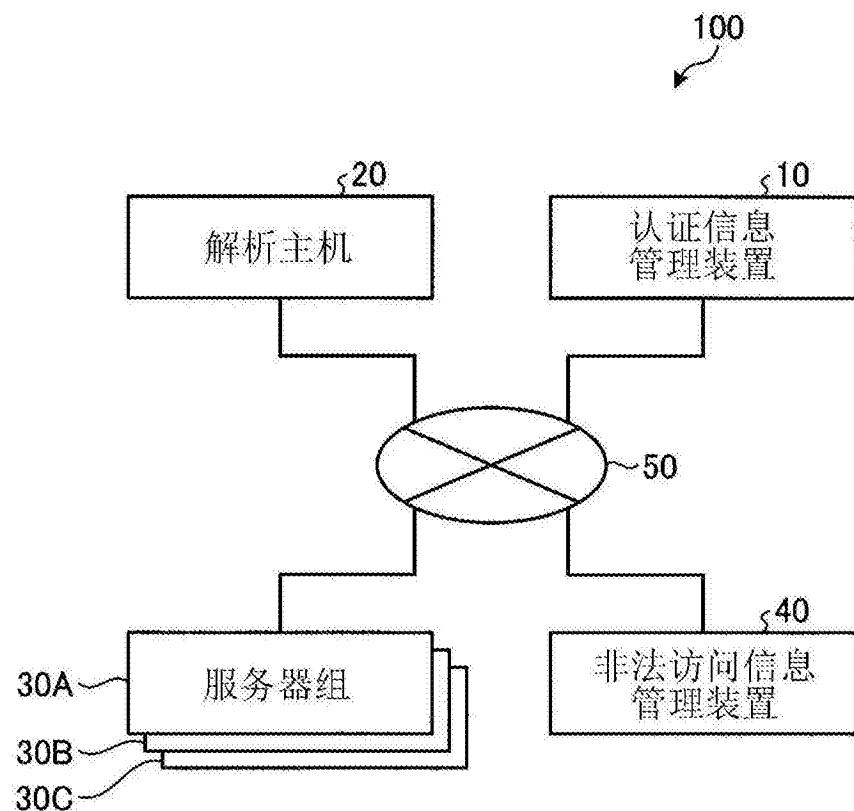


图1

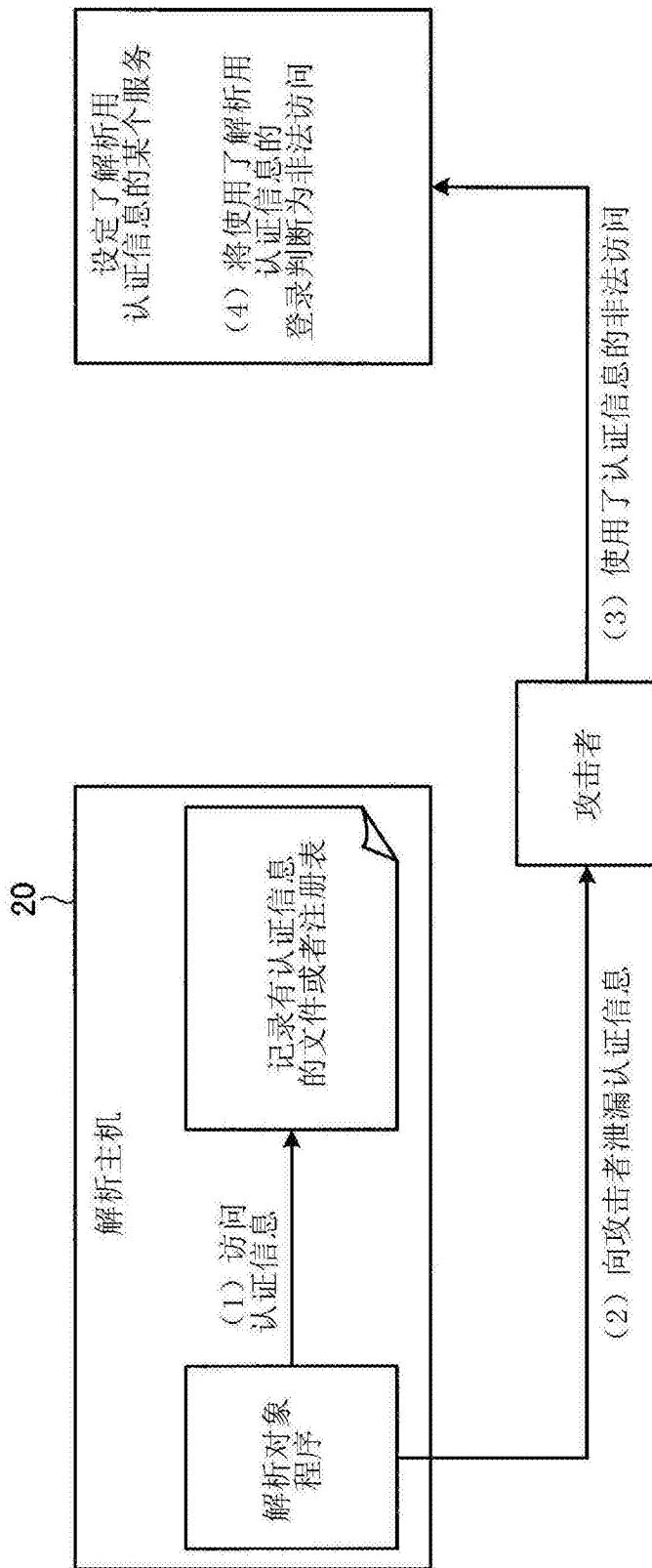


图2

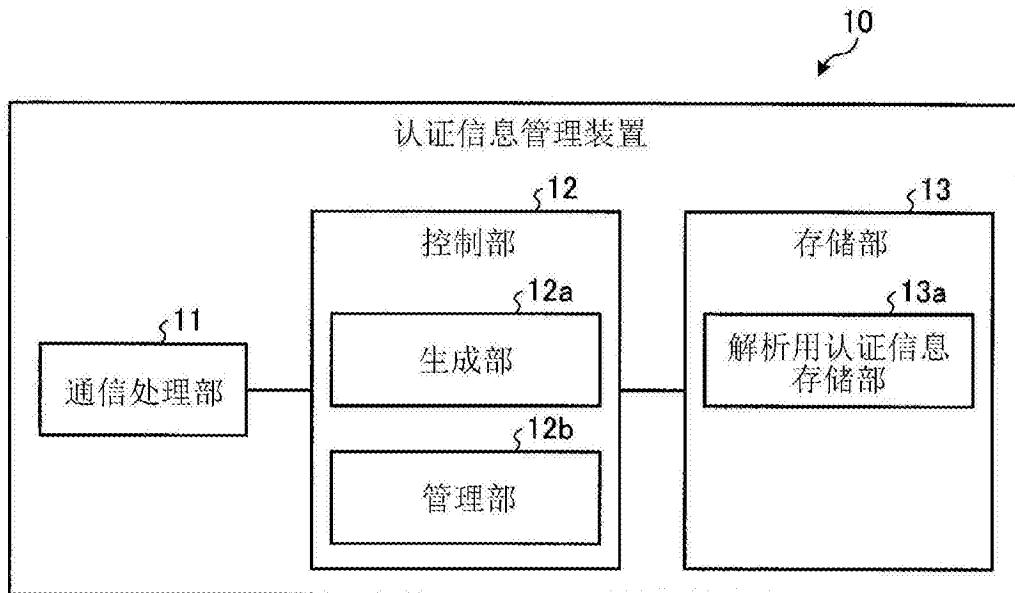


图3

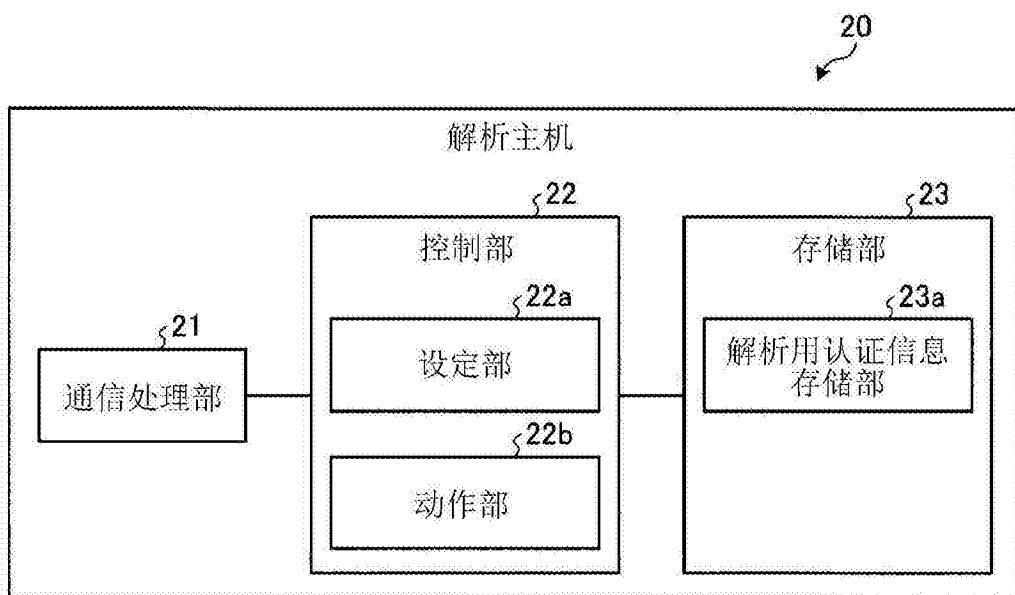


图4

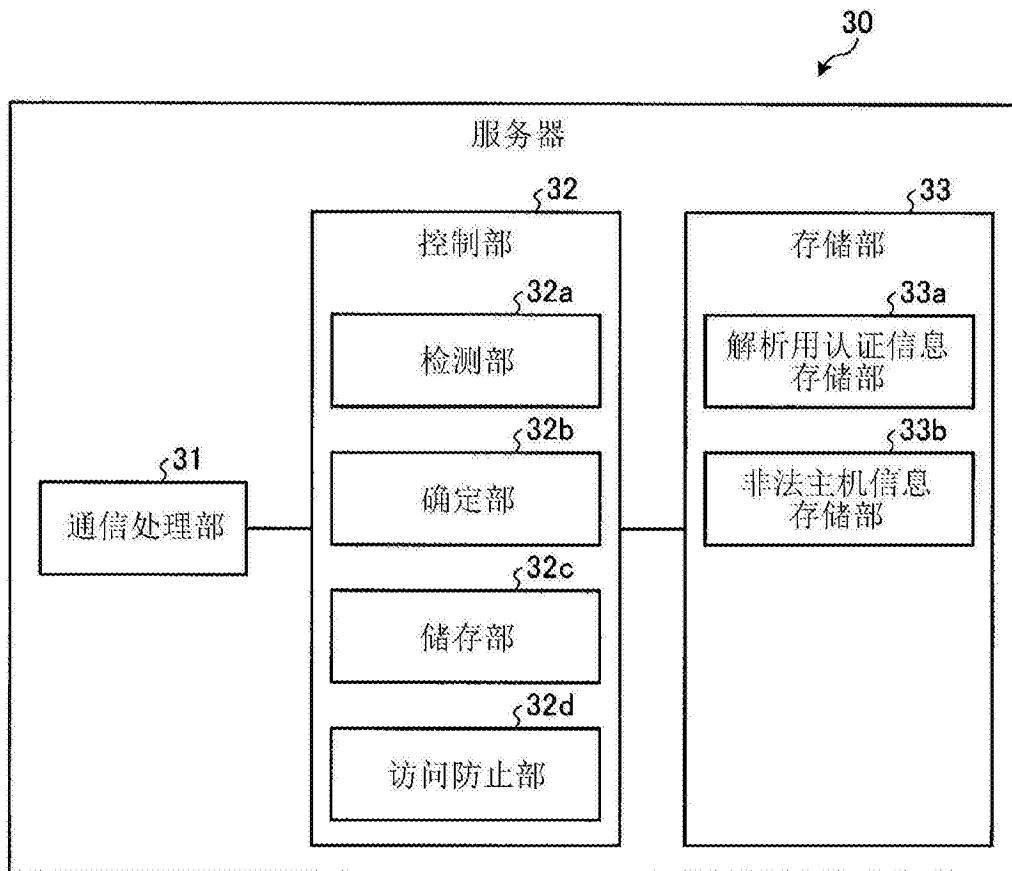


图5

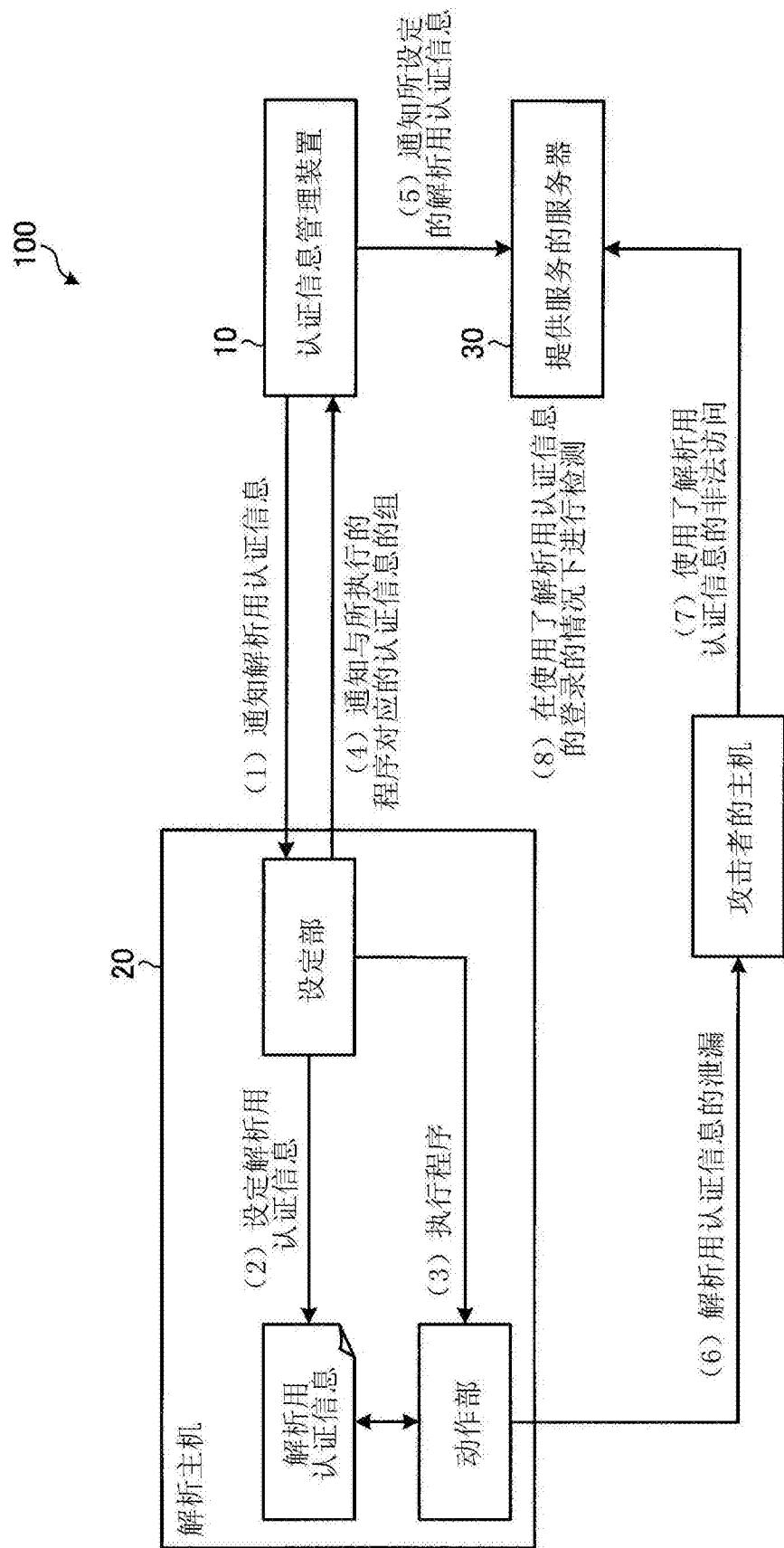


图6

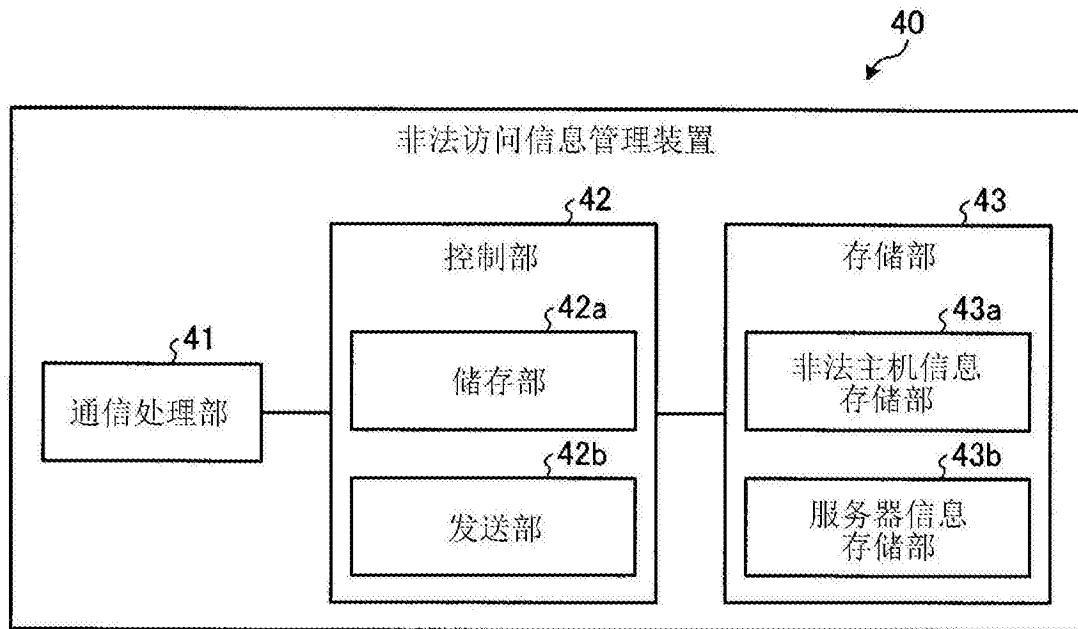


图7

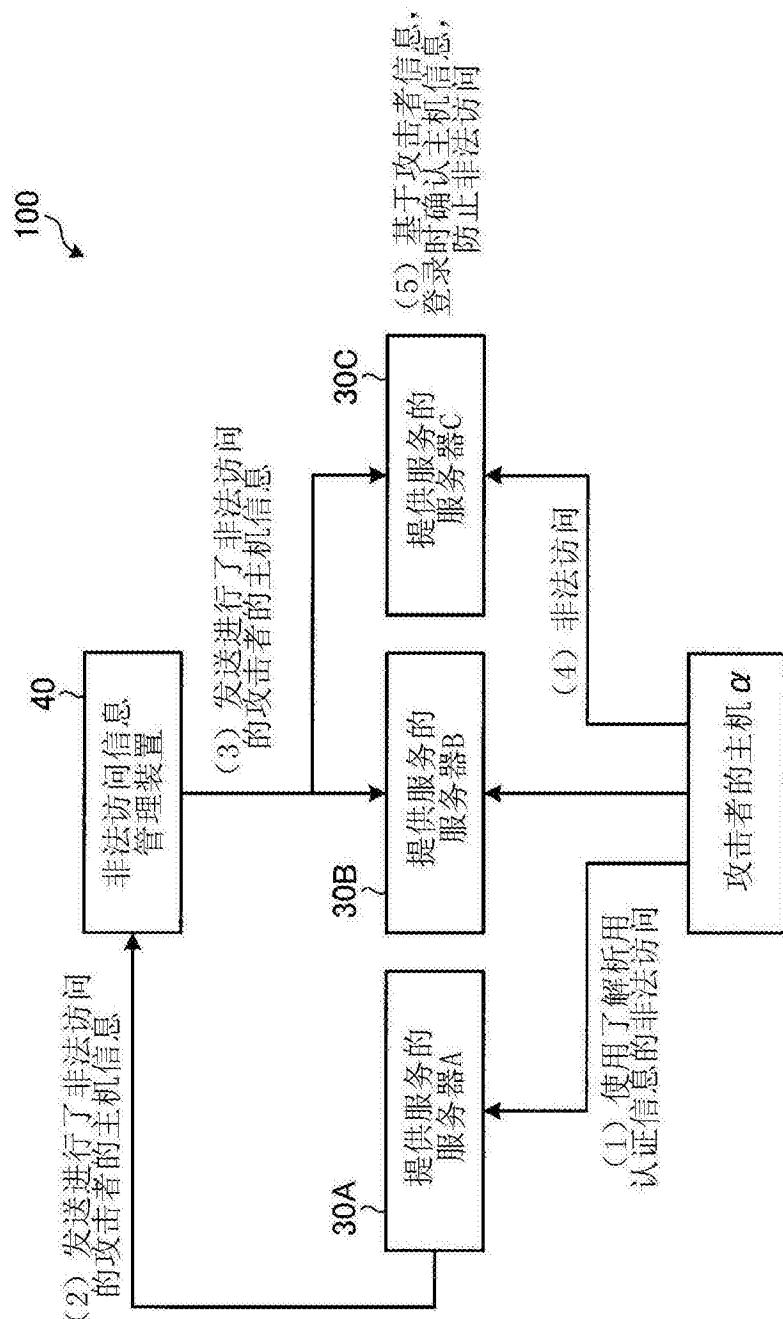


图8

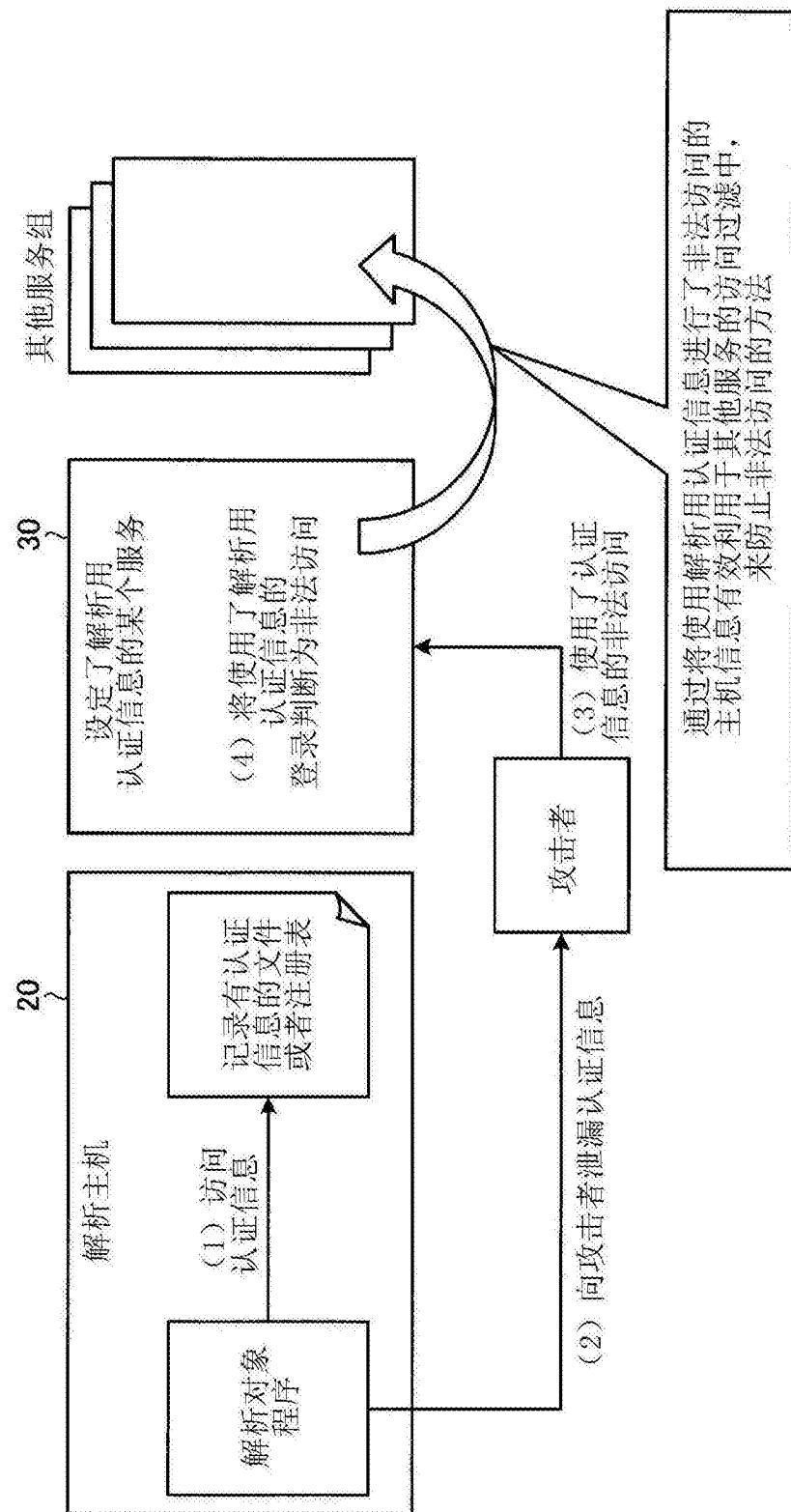


图9

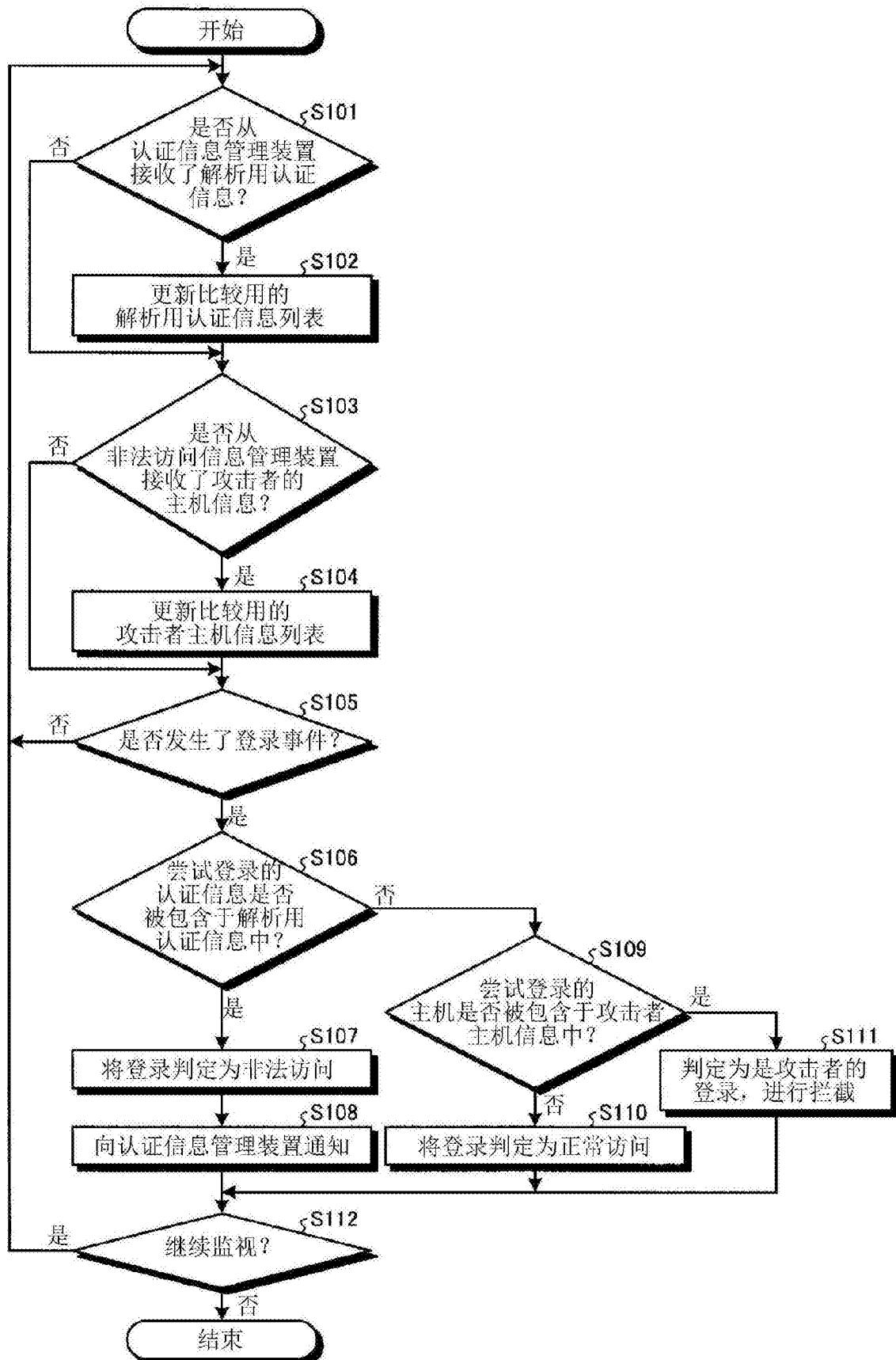


图10

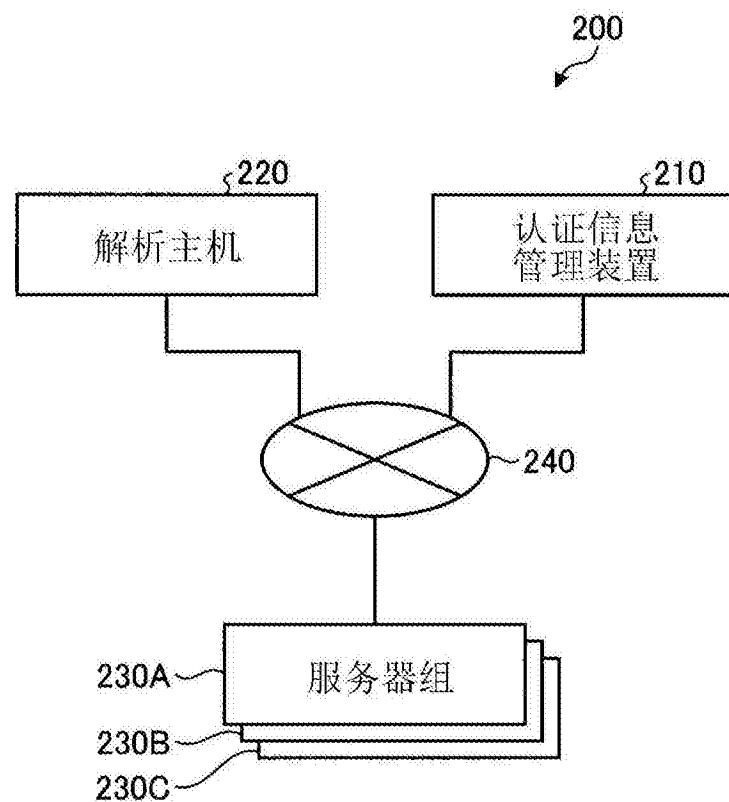


图11

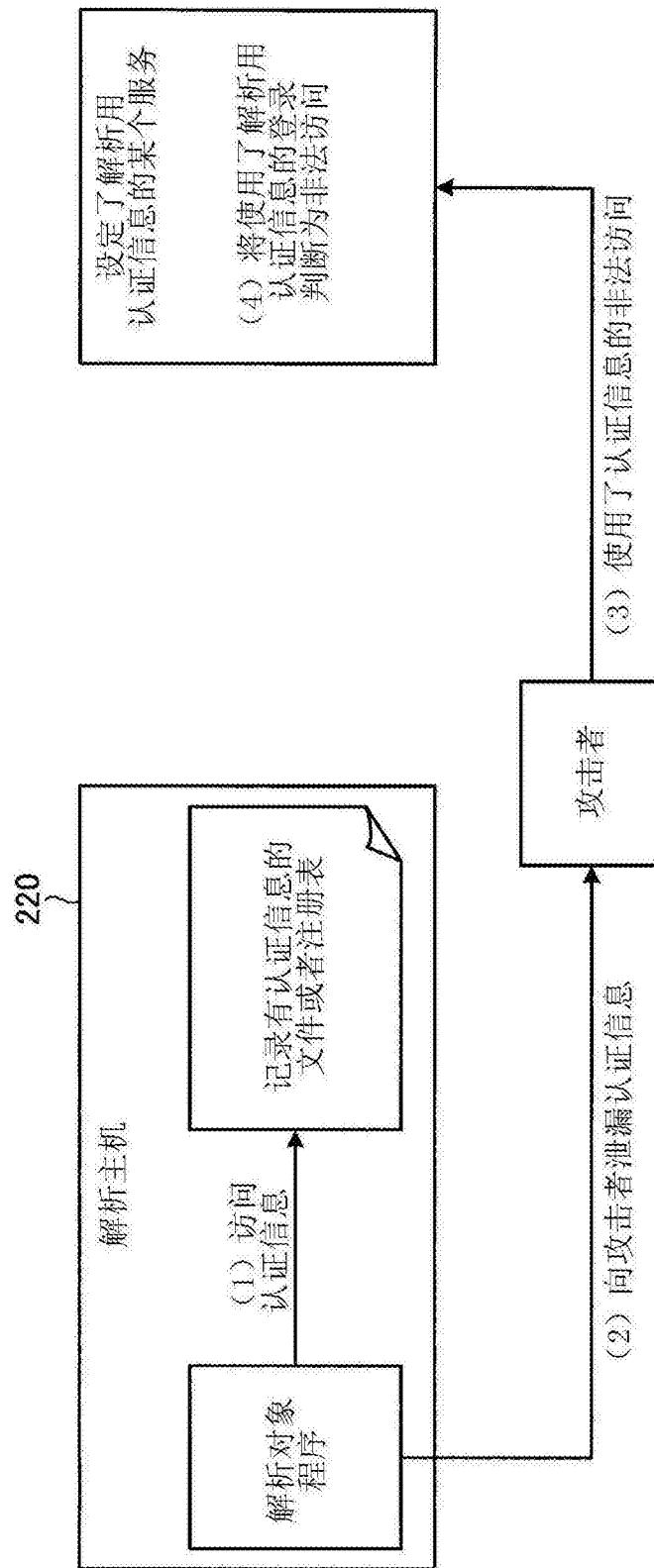


图12

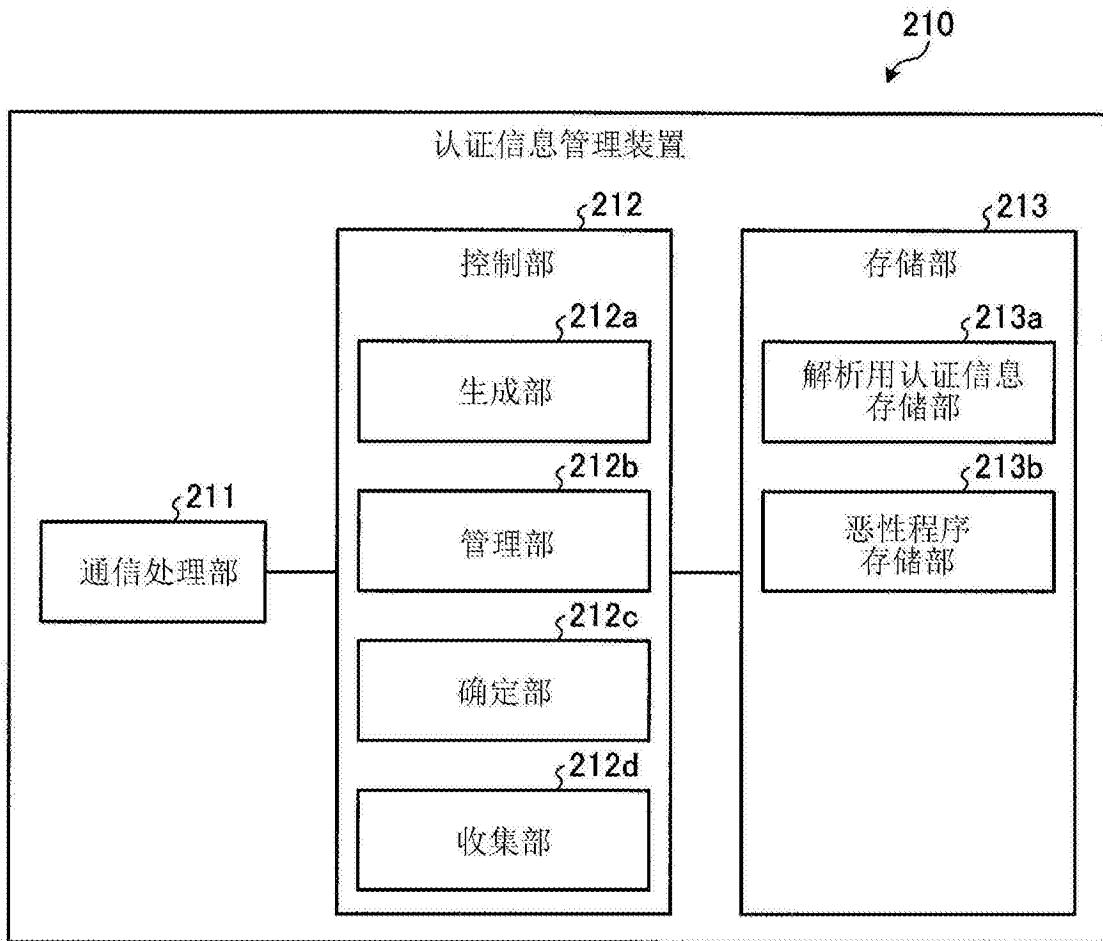


图13

解析程序	客户端 应用程序	认证信息
程序1	SSH	认证信息A
程序2	FTP	认证信息B
程序3	SSH	认证信息C
程序3	FTP	认证信息D
程序3	POP	认证信息E

图14

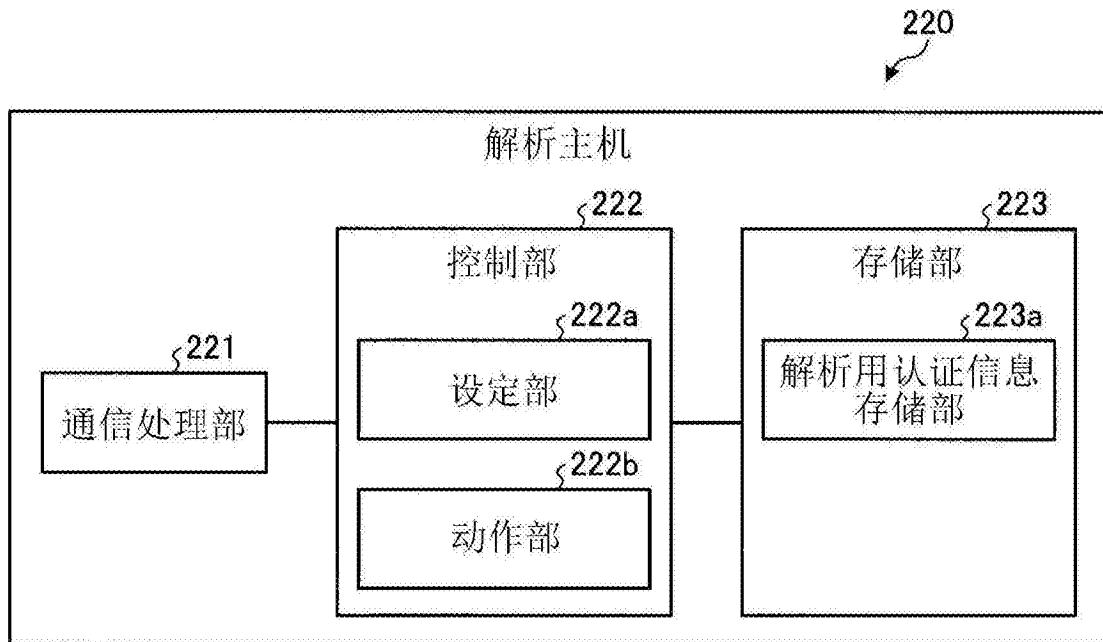


图15

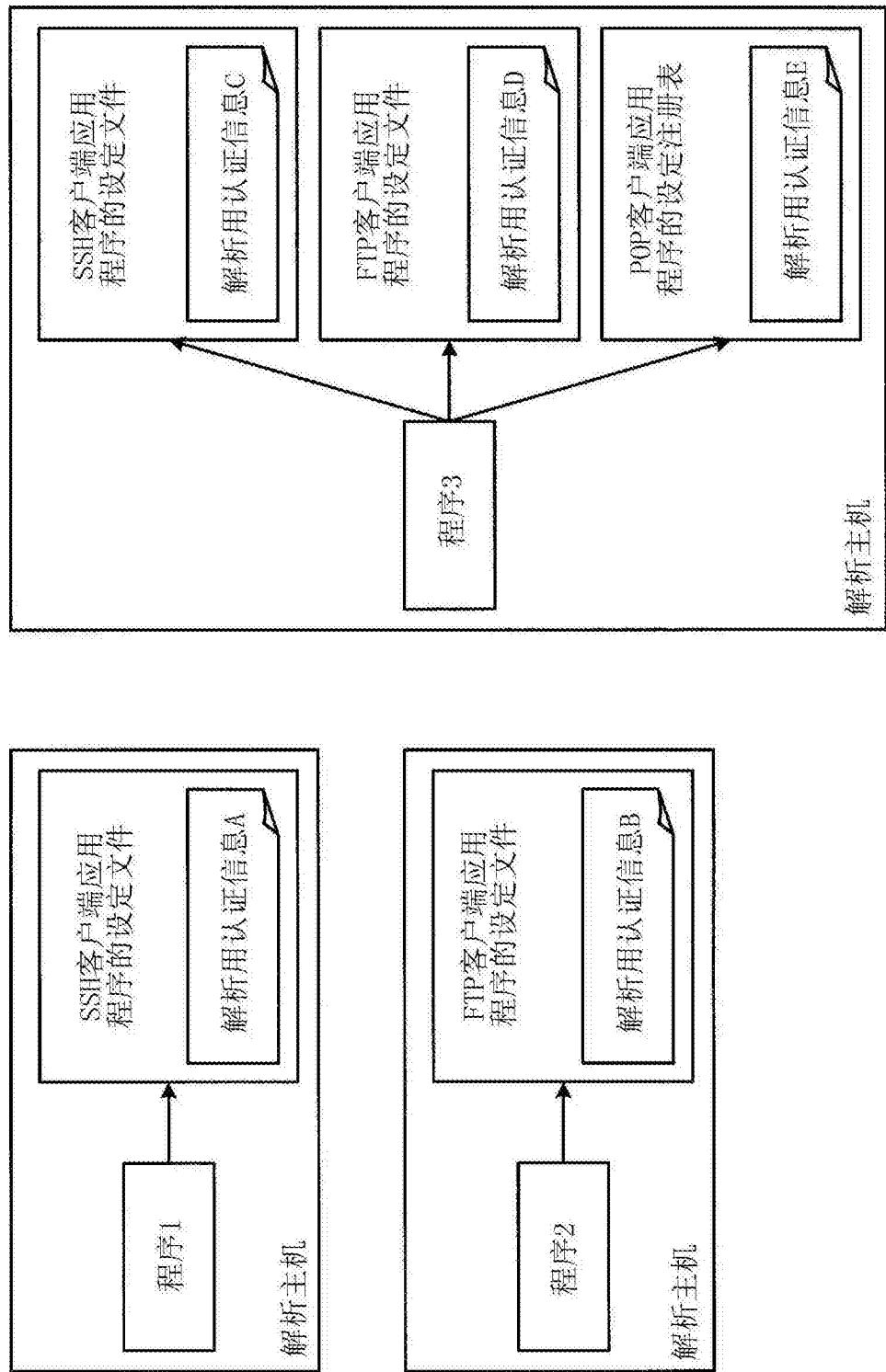


图 16

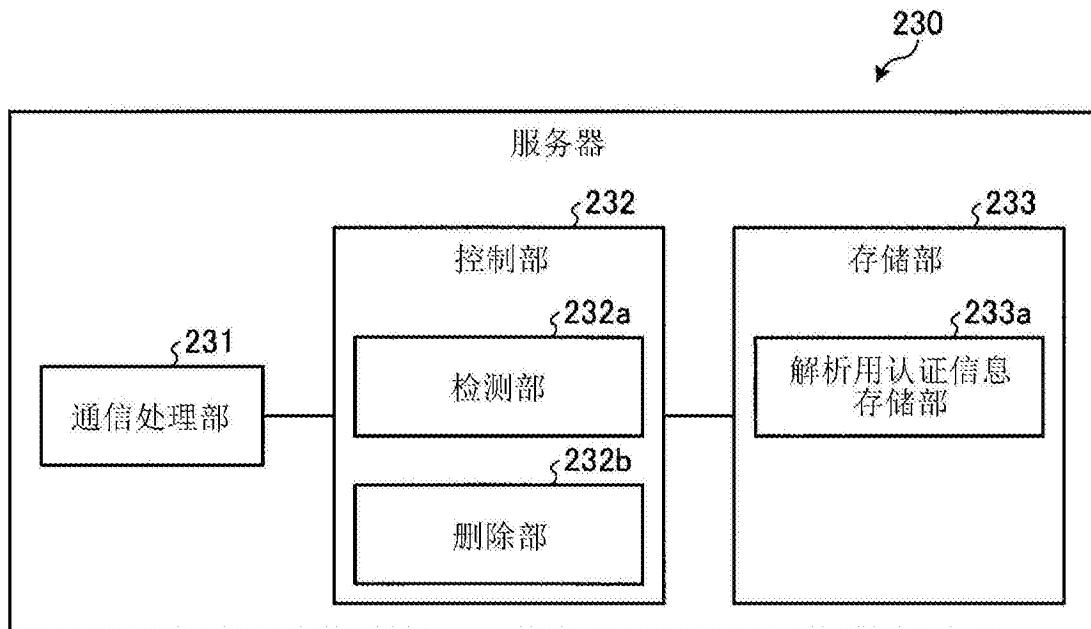


图17

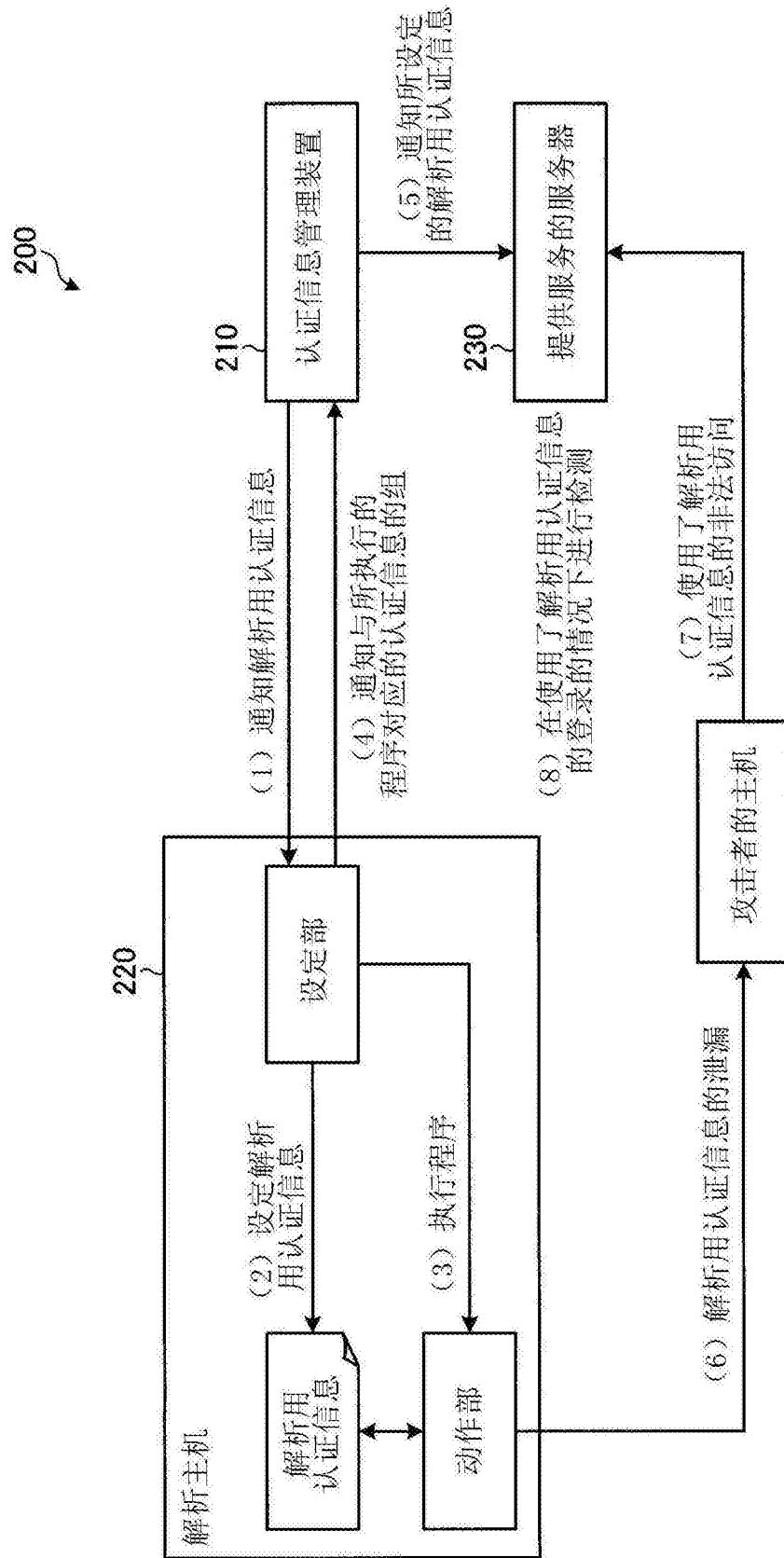


图18

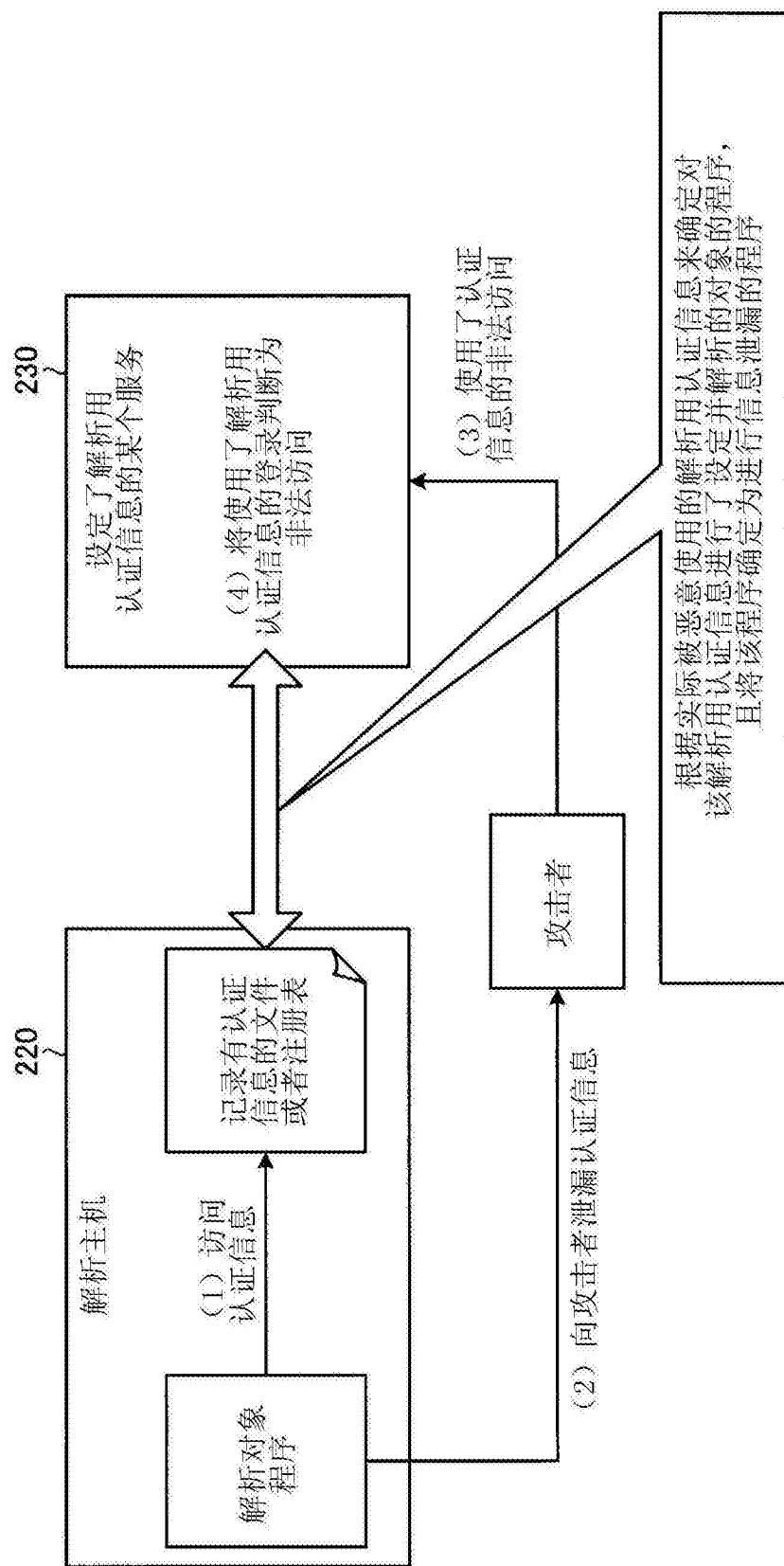


图19

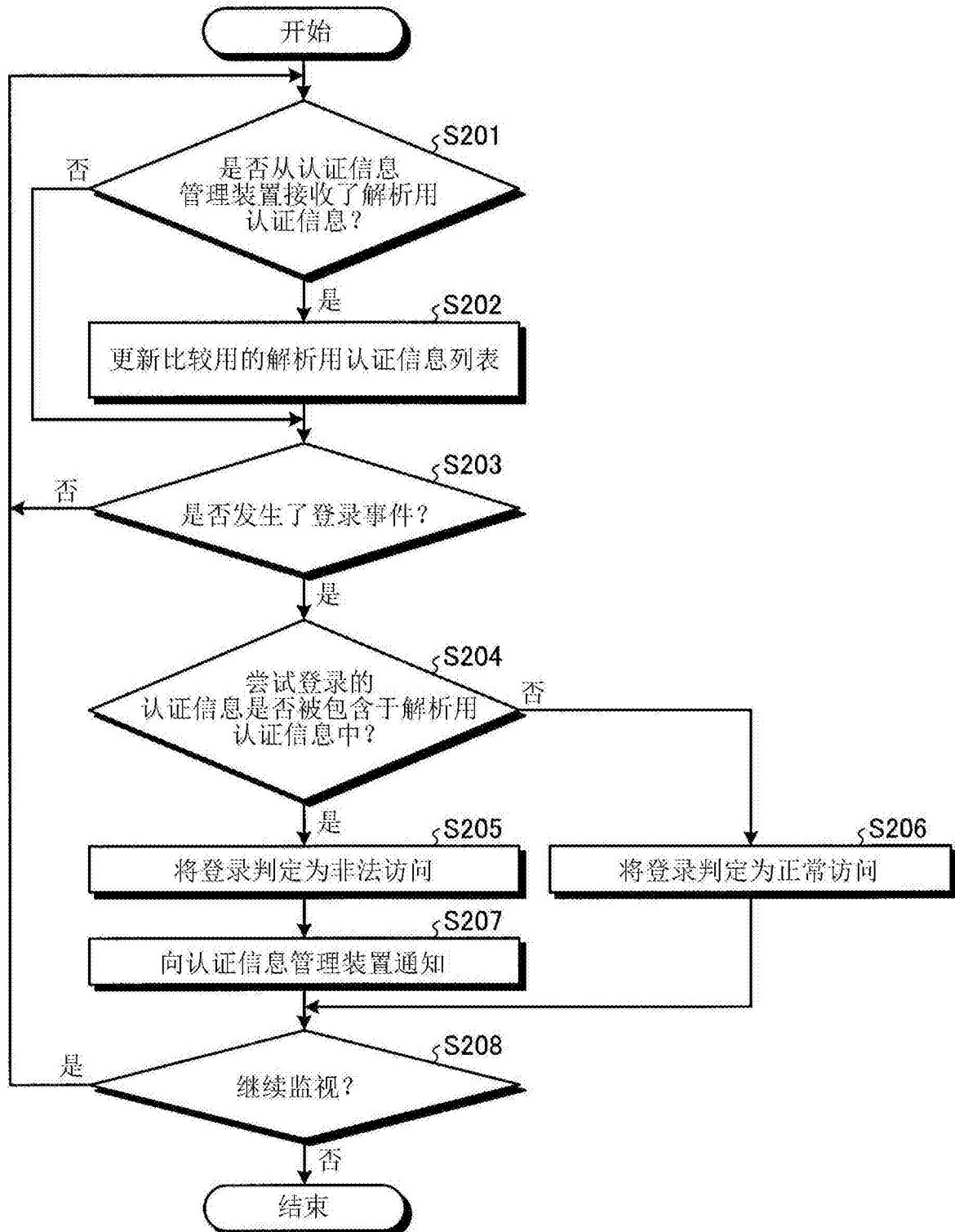


图20

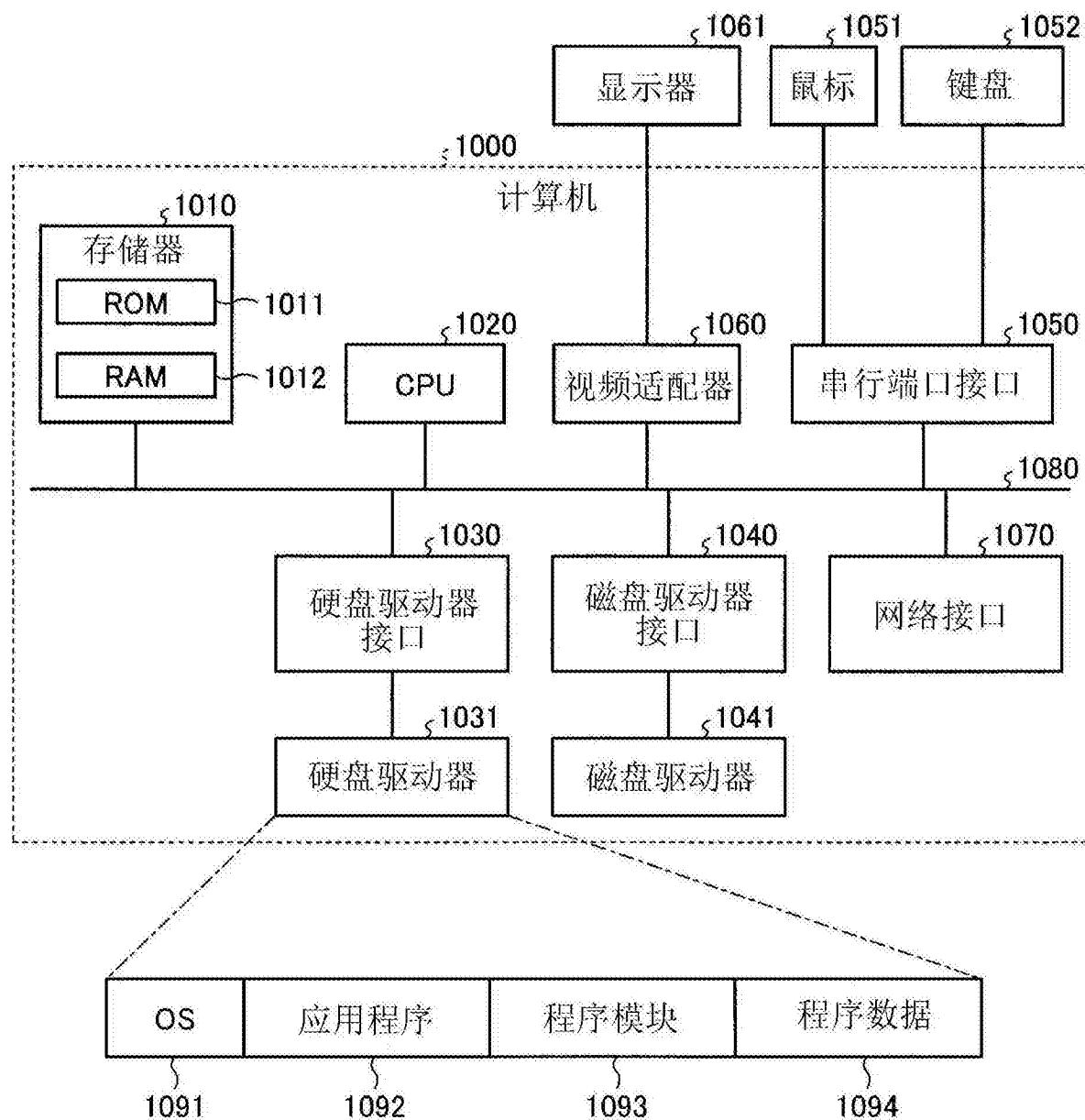


图21