



(12) 发明专利

(10) 授权公告号 CN 101965709 B

(45) 授权公告日 2013. 12. 11

(21) 申请号 200980108332.9

(22) 申请日 2009.03.05

(30) 优先权数据

2008-058884 2008. 03. 10 JP

(85) PCT申请进入国家阶段日

2010. 09. 09

(86) PCT 申请的申请数据

PCT/JP2009/054173 2009.03.05

(87) PCT申请的公布数据

W02009/113444 JA 2009.09.17

(73) 专利权人 三菱电机株式会社

地址 日本东京

(72)发明人 松田规 服部充洋 米田健

(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 11038

代理人 金春实

(51) Int. Cl.

H04L 9/08 (2006.01)

(56) 对比文件

CN 1607484 A, 2005. 04. 20.

CN 101004745 A, 2007. 07. 25,

Bruce Schneier 著. 高级门限方案. 《应用密码学 协议、算法与 C 源程序》. 2007,

王箭. 存储最优的传感器网络密钥共享. 《南京航空航天大学学报》. 2006, 第 38 卷 (第 6 期), 第 692-696 页.

肖亮亮等. 线性多密钥共享体制. 《中国科学 E 辑》. 2004, 第 34 卷 (第 10 期),

Adi Shamir. How to Share s Secret.

《Communication of the ACM》.1979, 第22卷(第11期), 第612-613页.

审查员 李媛

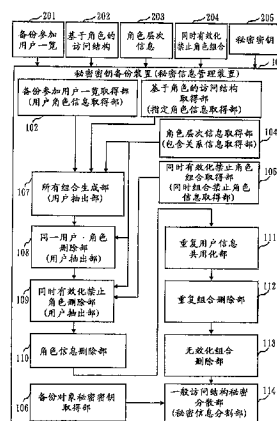
权利要求书4页 说明书22页 附图16页

(54) 发明名称

秘密信息管理装置、信息处理装置以及秘密
信息管理系统

(57) 摘要

即使在使用利用角色来指定了访问结构的基于角色的访问结构的情况下也安全地实现秘密密钥备份。所有组合生成部 107 取得作为备份参加用户的一览和该用户进行有效化的有效化角色的一览的备份参加用户一览 201、和作为可以复原秘密密钥 205 的指定角色的组合的基于角色的访问结构 202, 对指定角色应用备份参加用户一览 201 中记载的用户, 来生成作为有可能复原秘密密钥的用户的用户的所有组合的所有组合抽出结果, 同一用户・角色删除部 108 等从所有组合抽出结果中删除重复示出了同一用户的组合等, 一般访问结构秘密分散部 114 从秘密密钥生成秘密密钥片断, 对排除了重复的用户的组合分散秘密密钥片断。



1. 一种秘密信息管理装置,从多个用户中抽出成为从秘密信息分割的 2 个以上的分割秘密信息的管理者的用户,该秘密信息管理装置的特征在于,具有:

用户角色信息取得部,取得表示多个用户分别具备的角色的用户角色信息;

指定角色信息取得部,取得将 2 个以上的角色表示为指定角色的指定角色信息;以及

用户抽出部,对所述用户角色信息所表示的各用户的角色与所述指定角色信息所表示的各指定角色进行比较,针对每个指定角色抽出具备符合的角色的用户,按照指定角色的组合来对所抽出的用户进行组合,生成成为分割秘密信息的管理者的用户的组合,

所述秘密信息管理装置还具有秘密信息分割部,该秘密信息分割部根据由所述用户抽出部生成的成为分割秘密信息的管理者的用户的组合,生成分割秘密信息。

2. 根据权利要求 1 所述的秘密信息管理装置,其特征在于,

所述指定角色信息取得部存在取得对至少 2 个指定角色重复表示同一角色的指定角色信息的情况,

所述用户抽出部在所述指定角色信息重复表示同一角色的情况下,针对作为同一角色的至少 2 个指定角色分别抽出用户,并且从成为分割秘密信息的管理者的用户的组合中,去除对作为同一角色的至少 2 个指定角色分配了同一用户的组合。

3. 根据权利要求 1 所述的秘密信息管理装置,其特征在于,

所述用户角色信息取得部存在取得表示具备 2 个以上的角色的用户的用户角色信息的情况,

所述秘密信息管理装置还具有同时组合禁止角色信息取得部,该同时组合禁止角色信息取得部取得将禁止分配同一用户的 2 个以上的角色表示为同时组合禁止角色的同时组合禁止角色信息,

所述用户抽出部针对每个指定角色抽出用户,并且从成为分割秘密信息的管理者的用户的组合中,去除对与同时组合禁止角色相应的至少 2 个指定角色分配了同一用户的组合。

4. 根据权利要求 1 所述的秘密信息管理装置,其特征在于,

所述用户角色信息取得部存在取得表示具备上位角色的用户的用户角色信息的情况,其中,该上位角色包含 1 个以上的其他角色作为下位角色,

所述秘密信息管理装置还具有包含关系信息取得部,该包含关系信息取得部取得表示上位角色与下位角色的包含关系的包含关系信息,

所述用户抽出部根据包含关系信息所表示的包含关系,在指定角色信息中将某一个下位角色表示为指定角色的情况下,导出作为指定角色的下位角色的上位角色,抽出具备与作为指定角色的下位角色符合的角色的用户,并且与该下位角色对应起来抽出具备与作为指定角色的下位角色的上位角色符合的角色的用户。

5. 根据权利要求 4 所述的秘密信息管理装置,其特征在于,

所述秘密信息管理装置还具有同时组合禁止角色信息取得部,该同时组合禁止角色信息取得部取得将禁止分配同一用户的 2 个以上的角色表示为同时组合禁止角色的同时组合禁止角色信息,

所述用户抽出部在下位角色包含于同时组合禁止角色中的情况下,从成为分割秘密信息的管理者的用户的组合中,去除对同时组合禁止角色中包含的下位角色的上位角色以及

同时组合禁止角色中包含的其他某一个指定角色分配了同一用户的组合。

6. 根据权利要求 1 所述的秘密信息管理装置,其特征在於,

所述用户抽出部生成将所生成的用户的组合与各用户具备的角色一起表示的组合抽出信息,

所述秘密信息管理装置还具有:

角色信息删除部,从所述组合抽出信息中删除各用户的角色的信息;

重复用户信息共用化部,在所述组合抽出信息中存在重复组合了相同用户的组合的情况下,从该组合中去除用户的重复;

重复组合删除部,在所述组合抽出信息中存在仅用户的显示顺序不同而组合了相同用户的 2 个以上的组合的情况下,去除所重复的组合;以及

无效化组合删除部,在所述组合抽出信息中,某一个用户的组合包含于其他用户的组合中的情况下,去除包含于其他组合中的组合。

7. 一种信息处理装置,具有:

访问控制策略信息取得部,取得表示执行者角色与 1 个以上的许可者角色的多个组合的访问控制策略信息,其中,该执行者角色是被许可针对限制了访问的秘密信息的访问的角色,该许可者角色是对所述执行者角色许可针对所述秘密信息的访问的角色;

执行用户信息取得部,取得执行用户信息,该执行用户信息将执行针对所述秘密信息的访问的执行用户所具备的 1 个以上的角色表示为执行用户角色;

许可用户信息取得部,取得许可用户信息,该许可用户信息将对所述执行用户许可了针对所述秘密信息的访问的许可用户所具备的 1 个以上的角色表示为许可用户角色;

组合抽出部,该组合抽出部抽出在所述访问控制策略信息所表示的组合中的如下组合:执行者角色与所述执行用户信息所表示的执行用户角色一致、且各许可者角色与所述许可用户信息所表示的许可用户角色中的某一个一致的组合;该组合抽出部根据抽出的组合所表示的角色,生成指定角色信息,其中,该指定角色信息将从所述秘密信息分割的 2 个以上的分割秘密信息的管理者的角色表示为指定角色;

用户角色信息取得部,取得表示多个用户分别具备的角色的用户角色信息;

指定角色信息取得部,取得由所述组合抽出部生成的指定角色信息;

用户抽出部,对所述用户角色信息所表示的各用户的角色与所述指定角色信息所表示的各指定角色进行比较,针对每个指定角色抽出具备符合的角色的用户,按照指定角色的组合来对所抽出的用户进行组合,生成成为分割秘密信息的管理者的用户的组合;以及

秘密信息分割部,根据由所述用户抽出部生成的成为分割秘密信息的管理者的用户的组合,生成分割秘密信息。

8. 根据权利要求 7 所述的信息处理装置,其特征在於,

所述执行用户信息取得部存在如下情况:取得作为执行用户角色表示将 1 个以上的其他角色包含为下位角色的上位角色的执行用户信息的情况,

所述信息处理装置还具有包含关系信息取得部,该包含关系信息取得部取得表示上位角色与下位角色的包含关系的包含关系信息,

所述组合抽出部根据所述包含关系信息所表示的包含关系,判断执行者角色是否与执行用户角色的下位角色相应,在执行者角色与执行用户角色的下位角色相应的情况下,判

断和该执行者角色所组合的各许可者角色是否与许可用户角色中的某一个一致。

9. 根据权利要求 7 所述的信息处理装置,其特征在于,

所述许可用户信息取得部存在如下情况:取得作为许可用户角色表示将 1 个以上的其他角色包含为下位角色的上位角色的许可用户信息的情况,

所述信息处理装置还具有包含关系信息取得部,该包含关系信息取得部取得表示上位角色与下位角色的包含关系的包含关系信息,

所述组合抽出部根据所述包含关系信息所表示的包含关系,判断各许可者角色是否与许可用户角色的下位角色相应,并抽出如下组合:所有许可者角色的至少一部分与许可用户角色的下位角色相应、且剩余的许可者角色与许可用户角色一致的组合。

10. 根据权利要求 7 所述的信息处理装置,其特征在于,

所述组合抽出部根据抽出的组合所表示的角色,生成指定角色信息,该指定角色信息将从所述秘密信息分割的 2 个以上的分割秘密信息的管理者的角色表示为指定角色。

11. 一种信息处理装置,具有:

访问控制策略信息取得部,取得表示执行者角色与 1 个以上的许可者角色的多个组合的访问控制策略信息,其中,该执行者角色是被许可针对限制了访问的秘密信息的访问的角色,该许可者角色是对所述执行者角色许可针对所述秘密信息的访问的角色;

执行用户信息取得部,取得执行用户信息,该执行用户信息将执行针对所述秘密信息的访问的执行用户所具备的 1 个以上的角色表示为执行用户角色;

许可用户信息取得部,取得许可用户信息,该许可用户信息将对所述执行用户许可了针对所述秘密信息的访问的许可用户所具备的 1 个以上的角色表示为许可用户角色;以及

组合抽出部,该组合抽出部抽出在所述访问控制策略信息所表示的组合中的如下组合:执行者角色以及各许可者角色与所述执行用户信息所表示的执行用户角色以及所述许可用户信息所表示的许可用户角色中的某一个一致的组合;该组合抽出部根据抽出的组合所表示的角色,生成指定角色信息,其中,该指定角色信息将从所述秘密信息分割的 2 个以上的分割秘密信息的管理者的角色表示为指定角色;

用户角色信息取得部,取得表示多个用户分别具备的角色的用户角色信息;

指定角色信息取得部,取得由所述组合抽出部生成的指定角色信息;

用户抽出部,对所述用户角色信息所表示的各用户的角色与所述指定角色信息所表示的各指定角色进行比较,针对每个指定角色抽出具备符合的角色的用户,按照指定角色的组合来对所抽出的用户进行组合,生成成为分割秘密信息的管理者的用户的组合;以及

秘密信息分割部,根据由所述用户抽出部生成的成为分割秘密信息的管理者的用户的组合,生成分割秘密信息。

12. 根据权利要求 11 所述的信息处理装置,其特征在于,

所述执行用户信息取得部存在如下情况:取得作为执行用户角色表示将 1 个以上的其他角色包含为下位角色的上位角色的执行用户信息的情况,

所述许可用户信息取得部存在如下情况:取得作为许可用户角色表示将 1 个以上的其他角色包含为下位角色的上位角色的许可用户信息的情况,

所述信息处理装置还具有包含关系信息取得部,该包含关系信息取得部取得表示上位角色与下位角色的包含关系的包含关系信息,

所述组合抽出部根据所述包含关系信息所表示的包含关系,判断执行者角色以及各许可者角色是否与执行用户角色的下位角色以及许可用户角色的下位角色中的某一个相应,并抽出如下组合:执行者角色以及所有许可者角色的至少一部分与执行用户角色的下位角色以及许可用户角色的下位角色中的某一个相应、且执行者角色以及所有许可者角色中的剩余部分与执行用户角色以及许可用户角色中的某一个一致的组合。

秘密信息管理装置、信息处理装置以及秘密信息管理系统

技术领域

[0001] 本发明涉及用于分散并管理秘密密钥的技术。

背景技术

[0002] 以往,使用秘密分散技术来实施了秘密密钥备份方式。

[0003] 这是如下技术:通过将秘密密钥分割成多个秘密密钥片断,并由多个管理者分别保管各秘密密钥片断,可以秘密地保持秘密密钥的内容,并且安全地进行备份(例如,非专利文献 1)。

[0004] 在该方式中,除了将秘密密钥分割成几个这样的分割数 N 、即管理者的人数以外,还可以指定如果将其中的几个秘密密钥片断(管理者)到齐则能够复原秘密密钥这样的可复原数 k ,所以具有例如通过设为 $k < N$,即使一个管理者丢失了秘密密钥片断,也可以复原秘密密钥这样的特征。

[0005] 另外,还提出了如下秘密分散技术:通过研究将所分割的秘密密钥片断分发给管理者的分发方法,可以通过任意的管理者的组合来复原秘密密钥(例如,专利文献 1)。

[0006] 在该方式中,在存在 N 个管理者 $P1 \sim PN$ 时,指定如下访问结构:指定了可以通过哪个管理者具有的秘密密钥片断的组合来复原秘密密钥的访问结构。

[0007] 例如,在存在 3 名 ($P1$ 、 $P2$ 、 $P3$) 管理者时,表示在秘密密钥复原中需要 2 名管理者具有的秘密密钥片断,且其中的一人是管理者 $P1$ 的情况下,如 $\{\{P1, P2\}, \{P1, P3\}\}$ 那样指定访问结构。

[0008] 然后,根据访问结构对秘密密钥进行秘密分散,从而分割成 N 个秘密密钥片断。

[0009] 然后,对各管理者委托秘密密钥片断,从而仅在由访问结构指定的组合的管理者到齐时,可以复原秘密密钥。

[0010] 另一方面,在近年来的企业内信息系统中,正在利用基于角色的访问控制(Role-Based Access Control, RBAC)(例如,非专利文献 2)。

[0011] 这是根据工作上的作用、组织结构来规定角色,并对角色指定访问权限的构造。

[0012] 进而,通过使角色具有层次结构,可以进行权限的继承。

[0013] 另外,通过对角色登记用户,可以进行针对用户的访问控制。

[0014] 即使产生了人事变动,仅变更针对角色的用户登记即可,所以适合于企业内信息系统。

[0015] 例如,作为角色,制作部长角色、科长角色,对部长角色提供进行结算的权限,对科长角色提供制作付款单据的权限。然后,在部长角色中登记用户“田中部长”,在科长角色中登记用户“铃木科长”和“佐藤科长”。由此,能够进行铃木科长、佐藤科长可以制作付款单据,田中部长可以进行结算这样的访问控制。另外,通过使部长角色继承科长角色的权限,可以使田中部长也能够实施单据制作。另外,在高桥成为新科长的情况下,可以仅通过在科长角色中登记高桥科长,来简单地修正访问权限。

[0016] 专利文献 1:日本特开 2002-217891 号公报第 5 页~10 页

[0017] 非专利文献1 :A. Shamir“How to Share a Secret”Communications of the ACM、v. 22n. 11、p. 612-613、Nov. 1979

[0018] 非专利文献2 :David F. Ferraiolo、D. Richard Kuhn、Ramaswamy Chandramouli 著“Role-Based AccessControl”ARTECH HOUSE、INC.、2003 年、P6 ~ 16

发明内容

[0019] 在以往的秘密密钥备份方式中,在存在 N 个管理者 P1 ~ PN 时,指定了可以通过哪个管理者具有的秘密密钥片断的组合来复原秘密密钥。

[0020] 但是,由于在企业内信息系统中正在采用 RBAC,所以考虑关于秘密密钥备份也使用由 RBAC 规定的角色来指定访问结构。

[0021] 此处,由于一般对角色登记多个管理者,所以有可能在访问结构中重复指定角色这一点与以往不同。

[0022] 在以往的秘密分散方式中,以由访问结构指定的管理者 P1 ~ PN 是不同的管理者为前提,所以没有设想对访问结构的管理者的组合指定同一角色。

[0023] 因此,在重复指定了同一角色时,存在无法判断如何进行秘密分散来生成秘密密钥片断,并按照什么样的组合将秘密密钥片断分发给管理者才好这样的课题。

[0024] 例如,在如果 1 名部长和 2 名科长具有的秘密密钥片断到齐则可以复原秘密密钥的情况下,作为访问结构指定为 { 部长角色、科长角色、科长角色 }。

[0025] 然后,设按照以往的秘密分散方式生成了部长用秘密密钥片断、科长用秘密密钥片断 A、科长用秘密密钥片断 B。

[0026] 此处,产生将科长用秘密密钥片断 A • B 应该按照什么样的组合分发给科长这样的问题。

[0027] 作为情形 1,在将科长用秘密密钥片断 A • B 这两方分别分发给铃木科长、佐藤科长、高桥科长的情况下,如果田中部长、和铃木 / 佐藤 / 高桥科长中的某 1 名科长到齐,则秘密密钥片断到齐,所以可以对秘密密钥进行解密。

[0028] 这偏离了在 1 名部长和 2 名科长到齐的情况下才能对秘密密钥进行解密这样的条件,而可以通过更少的人数来复原秘密密钥,所以安全上并不优选。

[0029] 作为情形 2,考虑将科长用秘密密钥片断 A • B 中的某一个分发给各科长的情形。

[0030] 此处,设对铃木科长分发科长用秘密密钥片断 A,对佐藤 / 高桥科长分发秘密密钥片断 B。

[0031] 在该情况下,在田中部长、铃木科长、佐藤科长这 3 名到齐的情况下可以复原秘密密钥,但在田中部长、佐藤科长、高桥科长这 3 名中,秘密密钥片断不足,所以产生无法复原秘密密钥这样的问题。

[0032] 如上所述,存在如下课题:由以往的访问结构指定的管理者是以通过完全不同的管理者 P1 ~ PN 的组合来指定为前提,在指定了重复的角色的情况下,无法判断如何分发秘密密钥片断才好。

[0033] 本发明的主要目的之一为解决上述那样的课题,其主要目的在于,即使在使用利用角色指定了访问结构的基于角色的访问结构的情况下,也安全地实现秘密密钥备份。

[0034] 本发明的秘密信息管理装置,从多个用户中抽出成为从秘密信息分割的 2 个以上

的分割秘密信息的管理者的用户,该秘密信息管理装置的特征在于,具有:

[0035] 用户角色信息取得部,取得表示多个用户分别具备的角色的用户角色信息;

[0036] 指定角色信息取得部,取得将 2 个以上的角色表示为指定角色的指定角色信息;
以及

[0037] 用户抽出部,对所述用户角色信息所表示的各用户的角色与所述指定角色信息所表示的各指定角色进行比较,针对每个指定角色抽出具备符合的角色的用户,按照指定角色的组合来对所抽出的用户进行组合,生成成为分割秘密信息的管理者的用户的组合。

[0038] 其特征在于,所述指定角色信息取得部存在取得对至少 2 个指定角色重复表示同一角色的指定角色信息的情况,

[0039] 所述用户抽出部在所述指定角色信息重复表示同一角色的情况下,针对作为同一角色的至少 2 个指定角色分别抽出用户,并且从成为分割秘密信息的管理者的用户的组合中,去除对作为同一角色的至少 2 个指定角色分配了同一用户的组合。

[0040] 其特征在于,所述用户角色信息取得部存在取得表示具备 2 个以上的角色的用户的用户角色信息的情况,

[0041] 所述秘密信息管理装置还具有同时组合禁止角色信息取得部,该同时组合禁止角色信息取得部取得将禁止分配同一用户的 2 个以上的角色表示为同时组合禁止角色的同时组合禁止角色信息,

[0042] 所述用户抽出部针对每个指定角色抽出用户,并且从成为分割秘密信息的管理者的用户的组合中,去除对与同时组合禁止角色相应的至少 2 个指定角色分配了同一用户的组合。

[0043] 其特征在于,所述用户角色信息取得部存在取得表示具备上位角色的用户的用户角色信息的情况,其中,该上位角色包含 1 个以上的其他角色作为下位角色,

[0044] 所述秘密信息管理装置还具有包含关系信息取得部,该包含关系信息取得部取得表示上位角色与下位角色的包含关系的包含关系信息,

[0045] 所述用户抽出部根据包含关系信息所表示的包含关系,在指定角色信息中将某一个下位角色表示为指定角色的情况下,导出作为指定角色的下位角色的上位角色,抽出具备与作为指定角色的下位角色符合的角色的用户,并且与该下位角色对应起来抽出具备与作为指定角色的下位角色的上位角色符合的角色的用户。

[0046] 其特征在于,所述秘密信息管理装置还具有同时组合禁止角色信息取得部,该同时组合禁止角色信息取得部取得将禁止分配同一用户的 2 个以上的角色表示为同时组合禁止角色的同时组合禁止角色信息,

[0047] 所述用户抽出部在下位角色包含于同时组合禁止角色中的情况下,从成为分割秘密信息的管理者的用户的组合中,去除对同时组合禁止角色中包含的下位角色的上位角色以及同时组合禁止角色中包含的其他某一个指定角色分配了同一用户的组合。

[0048] 其特征在于,所述秘密信息管理装置还具有秘密信息分割部,该秘密信息分割部根据由所述用户抽出部生成的成为分割秘密信息的管理者的用户的组合,生成分割秘密信息。

[0049] 本发明的信息处理装置,具有:访问控制策略信息取得部,取得表示执行者角色与 1 个以上的许可者角色的多个组合的访问控制策略信息,其中,该执行者角色是被许可针对

限制了访问的秘密信息的访问的角色,该许可者角色是对所述执行者角色许可针对所述秘密信息的访问的角色;

[0050] 执行用户信息取得部,取得执行用户信息,该执行用户信息将执行针对所述秘密信息的访问的执行用户所具备的 1 个以上的角色表示为执行用户角色;

[0051] 许可用户信息取得部,取得许可用户信息,该许可用户信息将对所述执行用户许可了针对所述秘密信息的访问的许可用户所具备的 1 个以上的角色表示为许可用户角色;以及

[0052] 组合抽出部,抽出在所述访问控制策略信息所表示的组合中的如下组合:执行者角色与所述执行用户信息所表示的执行用户角色一致、且各许可者角色与所述许可用户信息所表示的许可用户角色中的某一个一致的组合。

[0053] 其特征在于,所述执行用户信息取得部存在如下情况:取得作为执行用户角色表示将 1 个以上的其他角色包含为下位角色的上位角色的执行用户信息的情况,

[0054] 所述信息处理装置还具有包含关系信息取得部,该包含关系信息取得部取得表示上位角色与下位角色的包含关系的包含关系信息,

[0055] 所述组合抽出部根据所述包含关系信息所表示的包含关系,判断执行者角色是否与执行用户角色的下位角色相应,在执行者角色与执行用户角色的下位角色相应的情况下,判断和该执行者角色所组合的各许可者角色是否与许可用户角色中的某一个一致。

[0056] 其特征在于,所述许可用户信息取得部存在如下情况:取得作为许可用户角色表示将 1 个以上的其他角色包含为下位角色的上位角色的许可用户信息的情况,

[0057] 所述信息处理装置还具有包含关系信息取得部,该包含关系信息取得部取得表示上位角色与下位角色的包含关系的包含关系信息,

[0058] 所述组合抽出部根据所述包含关系信息所表示的包含关系,判断各许可者角色是否与许可用户角色的下位角色相应,并抽出如下组合:所有许可者角色的至少一部分与许可用户角色的下位角色相应、且剩余的许可者角色与许可用户角色一致的组合。

[0059] 本发明的信息处理装置,具有:

[0060] 访问控制策略信息取得部,取得表示执行者角色与 1 个以上的许可者角色的多个组合的访问控制策略信息,其中,该执行者角色是被许可针对限制了访问的秘密信息的访问的角色,该许可者角色是对所述执行者角色许可针对所述秘密信息的访问的角色;

[0061] 执行用户信息取得部,取得执行用户信息,该执行用户信息将执行针对所述秘密信息的访问的执行用户所具备的 1 个以上的角色表示为执行用户角色;

[0062] 许可用户信息取得部,取得许可用户信息,该许可用户信息将对所述执行用户许可了针对所述秘密信息的访问的许可用户所具备的 1 个以上的角色表示为许可用户角色;以及

[0063] 组合抽出部,抽出在所述访问控制策略信息所表示的组合中的如下组合:执行者角色以及各许可者角色与所述执行用户信息所表示的执行用户角色以及所述许可用户信息所表示的许可用户角色中的某一个一致的组合。

[0064] 其特征在于,所述执行用户信息取得部存在如下情况:取得作为执行用户角色表示将 1 个以上的其他角色包含为下位角色的上位角色的执行用户信息的情况,

[0065] 所述许可用户信息取得部存在如下情况:取得作为许可用户角色表示将 1 个以上

的其他角色包含为下位角色的上位角色的许可用户信息的情况，

[0066] 所述信息处理装置还具有包含关系信息取得部，该包含关系信息取得部取得表示上位角色与下位角色的包含关系的包含关系信息，

[0067] 所述组合抽出部根据所述包含关系信息所表示的包含关系，判断执行者角色以及各许可者角色是否与执行用户角色的下位角色以及许可用户角色的下位角色中的某一个相应，并抽出如下组合：执行者角色以及所有许可者角色的至少一部分与执行用户角色的下位角色以及许可用户角色的下位角色中的某一个相应、且执行者角色以及所有许可者角色中的剩余部分与执行用户角色以及许可用户角色中的某一个一致的组合。

[0068] 其特征在于，所述组合抽出部根据抽出的组合所表示的角色，生成指定角色信息，该指定角色信息将从所述秘密信息分割的 2 个以上的分割秘密信息的管理者的角色表示为指定角色。

[0069] 本发明的秘密信息管理系统，具有：

[0070] 访问控制策略信息取得部，取得表示执行者角色与 1 个以上的许可者角色的多个组合的访问控制策略信息，其中，该执行者角色是被许可针对限制了访问的秘密信息的访问的角色，该许可者角色是对所述执行者角色许可针对所述秘密信息的访问的角色；

[0071] 执行用户信息取得部，取得执行用户信息，该执行用户信息将执行针对所述秘密信息的访问的执行用户所具备的 1 个以上的角色表示为执行用户角色；

[0072] 许可用户信息取得部，取得许可用户信息，该许可用户信息将对所述执行用户许可了针对所述秘密信息的访问的许可用户所具备的 1 个以上的角色表示为许可用户角色；

[0073] 组合抽出部，该组合抽出部抽出在所述访问控制策略信息所表示的组合中的如下组合：执行者角色与所述执行用户信息所表示的执行用户角色一致、且各许可者角色与所述许可用户信息所表示的许可用户角色中的某一个一致的组合；该组合抽出部根据抽出的组合所表示的角色，生成指定角色信息，其中，该指定角色信息将从所述秘密信息分割的 2 个以上的分割秘密信息的管理者的角色表示为指定角色；

[0074] 用户角色信息取得部，取得表示多个用户分别具备的角色的用户角色信息；

[0075] 指定角色信息取得部，取得由所述组合抽出部生成的指定角色信息；

[0076] 用户抽出部，对所述用户角色信息所表示的各用户的角色与所述指定角色信息所表示的各指定角色进行比较，针对每个指定角色抽出具备符合的角色的用户，按照指定角色的组合来对所抽出的用户进行组合，生成成为分割秘密信息的管理者的用户的组合；以及

[0077] 秘密信息分割部，根据由所述用户抽出部生成的成为分割秘密信息的管理者的用户的组合，生成分割秘密信息。

[0078] 本发明的秘密信息管理系统，具有：

[0079] 访问控制策略信息取得部，取得表示执行者角色与 1 个以上的许可者角色的多个组合的访问控制策略信息，其中，该执行者角色是被许可针对限制了访问的秘密信息的访问的角色，该许可者角色是对所述执行者角色许可针对所述秘密信息的访问的角色；

[0080] 执行用户信息取得部，取得执行用户信息，该执行用户信息将执行针对所述秘密信息的访问的执行用户所具备的 1 个以上的角色表示为执行用户角色；

[0081] 许可用户信息取得部，取得许可用户信息，该许可用户信息将对所述执行用户许

可了针对所述秘密信息的访问的许可用户所具备的 1 个以上的角色表示为许可用户角色；以及

[0082] 组合抽出部,该组合抽出部抽出在所述访问控制策略信息所表示的组合中的如下组合:执行者角色以及各许可者角色与所述执行用户信息所表示的执行用户角色以及所述许可用户信息所表示的许可用户角色中的某一个一致的组合;该组合抽出部根据抽出的组合所表示的角色,生成指定角色信息,其中,该指定角色信息将从所述秘密信息分割的 2 个以上的分割秘密信息的管理者的角色表示为指定角色;

[0083] 用户角色信息取得部,取得表示多个用户分别具备的角色的用户角色信息;

[0084] 指定角色信息取得部,取得由所述组合抽出部生成的指定角色信息;

[0085] 用户抽出部,对所述用户角色信息所表示的各用户的角色与所述指定角色信息所表示的各指定角色进行比较,针对每个指定角色抽出具备符合的角色的用户,按照指定角色的组合来对所抽出的用户进行组合,生成成为分割秘密信息的管理者的用户的组合;以及

[0086] 秘密信息分割部,根据由所述用户抽出部生成的成为分割秘密信息的管理者的用户的组合,生成分割秘密信息。

[0087] 其特征在于,所述用户抽出部生成将所生成的用户的组合与各用户具备的角色一起表示的组合抽出信息,

[0088] 所述秘密信息管理装置还具有:

[0089] 角色信息删除部,从所述组合抽出信息中删除各用户的角色的信息;

[0090] 重复用户信息共用化部,在所述组合抽出信息中存在重复组合了相同用户的组合的情况下,从该组合中去除用户的重复;

[0091] 重复组合删除部,在所述组合抽出信息中存在仅用户的显示顺序不同而组合了相同用户的 2 个以上的组合的情况下,去除所重复的组合;以及

[0092] 无效化组合删除部,在所述组合抽出信息中,某一个用户的组合包含于其他用户的组合中的情况下,去除包含于其他组合中的组合。

[0093] 根据本发明,根据各用户具备的角色和指定角色的组合,抽出成为分割秘密信息的管理者的用户的组合,所以即使在使用利用角色来指定了访问结构的基于角色的访问结构的情况下,也可以安全地实现秘密密钥备份。

附图说明

[0094] 图 1 是示出实施方式 1 的秘密密钥备份装置的结构例的图。

[0095] 图 2 是示出实施方式 1 的备份参加用户一览的结构例的图。

[0096] 图 3 是示出实施方式 1 的备份参加用户一览的例子图。

[0097] 图 4 是示出实施方式 1 的基于角色的访问结构的结构例的图。

[0098] 图 5 是示出实施方式 1 的基于角色的访问结构的例子图。

[0099] 图 6 是示出实施方式 1 的角色层次信息的结构例的图。

[0100] 图 7 是示出实施方式 1 的角色层次信息的例子图。

[0101] 图 8 是示出实施方式 1 的同时有效化禁止角色组合的结构例的图。

[0102] 图 9 是示出实施方式 1 的同时有效化禁止角色组合的例子图。

- [0103] 图 10 是示出实施方式 1 的所抽出的可复原组合的结构例的图。
- [0104] 图 11 是示出实施方式 1 的所抽出的可复原组合（抽出全部组合）的例子的图。
- [0105] 图 12 是示出实施方式 1 的所抽出的可复原组合（同一用户・角色删除后）的例子的图。
- [0106] 图 13 是示出实施方式 1 的所抽出的可复原组合（同时有效化禁止角色删除后）的例子的图。
- [0107] 图 14 是示出实施方式 1 的所抽出的可复原组合（角色信息删除后）的例子的图。
- [0108] 图 15 是示出实施方式 1 的所抽出的可复原组合（重复用户信息共用化后）的例子的图。
- [0109] 图 16 是示出实施方式 1 的所抽出的可复原组合（重复组合删除后）的例子的图。
- [0110] 图 17 是示出实施方式 1 的所抽出的可复原组合（无效化组合删除后）的例子的图。
- [0111] 图 18 是示出实施方式 1 的秘密密钥备份装置的动作例的流程图。
- [0112] 图 19 是示出实施方式 1 的备份参加用户一览的例子的图。
- [0113] 图 20 是示出实施方式 1 的秘密密钥备份装置的硬件结构例的流程图。
- [0114] 图 21 是示出实施方式 2 的秘密密钥备份系统的结构例的图。
- [0115] 图 22 是示出实施方式 2 的备份许可用户一览的结构例的图。
- [0116] 图 23 是示出实施方式 2 的访问控制策略的结构例的图。
- [0117] 图 24 是示出实施方式 2 的访问控制策略的例子的图。
- [0118] 图 25 是示出实施方式 2 的备份执行用户信息的例子的图。
- [0119] 图 26 是示出实施方式 2 的秘密密钥备份系统的动作例的流程图。
- [0120] （附图标记说明）
- [0121] 101:秘密密钥备份装置;102:备份参加用户一览取得部;103:基于角色的访问结构取得部;104:角色层次信息取得部;105:同时有效化禁止角色组合取得部;106:备份对象秘密密钥取得部;107:所有组合生成部;108:同一用户・角色删除部;109:同时有效化禁止角色删除部;110:角色信息删除部;111:重复用户信息共用化部;112:重复组合删除部;113:无效化组合删除部;114:一般访问结构秘密分散部;2101:基于角色的访问结构生成装置;2102:访问控制策略;2103:备份执行用户信息;2104:备份许可用户一览;2105:访问控制策略取得部;2106:备份执行用户信息取得部;2107:备份许可用户一览取得部;2108:备份权限抽出部;2109:有效访问权限抽出部;2110:基于角色的访问结构生成部;3000:秘密密钥备份系统。

具体实施方式

[0122] （实施方式 1）

[0123] 在本实施方式中,说明如下技术:在使用利用角色来指定了访问结构的基于角色的访问结构的情况下,参照参加到备份中的用户、和由该用户进行有效化的有效化角色,得到与以往的访问结构同样地按照用户单位指定的基于用户的访问结构,从而使用以往的秘密分散技术来安全地实现秘密密钥备份。

[0124] 图 1 是本实施方式的秘密密钥备份装置 101 的功能结构图。

[0125] 秘密密钥备份装置 101 是从多个用户中抽出成为从秘密密钥（秘密信息）分割的 2 个以上的秘密密钥片断（分割秘密信息）的管理者的用户的装置，是秘密信息管理装置的例子。

[0126] 在图 1 中，备份参加用户一览取得部 102 取得：表示参加到备份中的用户的一览、和由该用户进行有效化的有效化角色的一览的备份参加用户一览信息 201（以下，称为备份参加用户一览 201）。

[0127] 在后面将详细叙述，备份参加用户一览 201 是如图 2 以及图 3 所示，表示多个用户分别进行有效化的角色的信息，是用户角色信息的例子。

[0128] 另外，备份参加用户一览取得部 102 是用户角色信息取得部的例子。

[0129] 基于角色的访问结构取得部 103 取得作为可以复原秘密密钥的角色的组合的基于角色的访问结构信息 202（以下，称为基于角色的访问结构 202）。

[0130] 在后面将详细叙述，基于角色的访问结构 202 是如图 4 以及图 5 所示，将 2 个以上的角色表示为可复原组合的信息，是指定角色信息的例子。

[0131] 另外，将可复原组合中包含的角色称为指定角色。

[0132] 基于角色的访问结构取得部 103 是指定角色信息取得部的例子。

[0133] 角色层次信息取得部 104 取得与在由 RBAC 规定的角色之间关联起来的层次结构相关的角色层次信息 203。

[0134] 在后面将详细叙述，角色层次信息 203 是如图 6 以及图 7 所示，表示上位角色与下位角色的包含关系的信息，是包含关系信息的例子。

[0135] 即，存在备份参加用户一览 201 中示出的用户的角色承袭了其他角色（作为下位角色而包含）的情况。

[0136] 这样，在某用户使承袭了其他角色的上位角色有效化的情况下，优选使上位的角色有效化的用户还能够利用下位角色的权限而使访问权限的管理变得容易。因此，使用示出了角色之间的承袭关系的角色层次信息 203。

[0137] 另外，角色层次信息取得部 104 是包含关系信息取得部的例子。

[0138] 同时有效化禁止角色组合取得部 105 取得表示用户不得同时进行有效化的角色的组合的同时有效化禁止角色组合信息 204（以下，称为同时有效化禁止角色组合 204）。

[0139] 在后面将详细叙述，同时有效化禁止角色组合 204 是如图 8 以及图 9 所示，将禁止同一用户同时进行有效化的 2 个以上的角色表示为同时有效化禁止角色（同时组合禁止角色）的信息，是同时组合禁止角色信息的例子。

[0140] 即，存在在备份参加用户一览 201 中出现使 2 个以上的角色有效化的用户的情况，在这样的情况下，为了不对 2 个以上的角色重复分配同一用户，使用示出了用户不得同时进行有效化的角色的组合的同时有效化禁止角色组合 204。

[0141] 另外，同时有效化禁止角色组合取得部 105 是同时组合禁止角色信息取得部的例子。

[0142] 另外，为了即使在某用户使承袭了其他角色的上位角色有效化的情况下，也不对 2 个以上的角色重复分配同一用户，需要考虑角色之间的承袭关系（包含关系）。因此，还对示出了角色之间的承袭关系的角色层次信息 203 进行对照，来判断是否相应于同时有效化禁止角色的组合。

[0143] 备份对象秘密密钥取得部 106 取得用户想要进行备份的秘密密钥 205。

[0144] 所有组合生成部 107 通过对基于角色的访问结构 202 中包含的角色应用备份参加用户一览 201 中记载的用户,生成作为有可能能够复原秘密密钥的用户的所有组合的、所有组合抽出结果。

[0145] 即,所有组合生成部 107 对备份参加用户一览 201 中示出的各用户的角色、与基于角色的访问结构 202 中示出的各指定角色进行比较,针对每个指定角色抽出使符合的角色有效化的用户,按照指定角色的组合来组合所抽出的用户,而生成成为秘密密钥片断的管理者的用户的组合。

[0146] 所有组合生成部 107 在将某下位角色作为指定角色而表示于基于角色的访问结构 202 中的情况下,导出作为指定角色的下位角色的上位角色,抽出使所导出的上位角色有效化的用户,并且与该下位角色对应起来抽出使上位角色有效化的用户。

[0147] 所有组合生成部 107 是用户抽出部的例子。

[0148] 同一用户・角色删除部 108,在所有组合抽出结果中,属于某角色的用户重复出现了的情况下,删除该条目,而生成同一用户・角色删除结果。

[0149] 即,存在在基于角色的访问结构 202 中对至少 2 个指定角色重复示出了同一角色的情况(在图 5 的例子中,组合编号 No1),在该情况下,所有组合生成部 107 对作为同一角色的 2 个以上的指定角色(RoleA 和 RoleA)分别抽出用户,但同一用户・角色删除部 108 去除对作为同一角色的 2 个以上的指定角色(RoleA 和 RoleA)分配了同一用户的组合。

[0150] 另外,如上所述,在下位角色是指定角色的情况下,所有组合生成部 107 还一并将该下位角色的上位角色也作为用户的抽出对象,但其结果,存在对作为同一角色的 2 个以上的指定角色分配同一用户的情况。

[0151] 例如,在 RoleD 是 RoleA 的上位角色,指定角色是“RoleA 和 RoleA”的情况下,对“RoleA 和 RoleA”,重复抽出与 RoleD 相应的同一用户,生成同一用户的组合。在这样的情况下,同一用户・角色删除部 108 也排除同一用户的组合。

[0152] 同时有效化禁止角色删除部 109,在同一用户・角色删除结果中,某用户使多个由同时有效化禁止角色组合 204 指定的组合的角色有效化的情况下,删除该条目,而生成同时有效化禁止角色删除结果。

[0153] 另外,在基于角色的访问结构 202 中,示出了不同的指定角色的组合(在图 5 的例子中,组合编号 No2)的情况下,在同一用户使多个角色有效化的情况下,即使是不同的指定角色,所有组合生成部 107 也重复抽出同一用户。在这样的情况下,同时有效化禁止角色删除部 109 去除对与同时有效化禁止角色组合 204 相应的 2 个以上的指定角色分配了同一用户的组合。

[0154] 另外,如上所述,在下位角色是指定角色的情况下,所有组合生成部 107 将该下位角色的上位角色也一并作为用户的抽出对象。此时,在同时有效化禁止角色组合 204 中示出了下位角色的情况下,同时有效化禁止角色删除部 109 去除对该上位角色和同时有效化禁止角色组合 204 的其他角色分配了同一用户的组合。

[0155] 另外,同一用户・角色删除部 108 也是用户抽出部的例子。

[0156] 角色信息删除部 110,虽然在同时有效化禁止角色删除结果中,还一并记载有用户所属的角色,但删除该角色信息,而生成角色信息删除结果。

[0157] 重复用户信息共用化部 111 在角色信息删除结果中的各条目中出现了同一用户的情况下,通过将其作为重复而去除,来生成重复用户信息共用化结果。

[0158] 重复组合删除部 112,在重复用户信息共用化结果中,去除仅用户信息的记载顺序不同而表示相同的用户的组合的重复组合,从而生成重复组合删除结果。

[0159] 无效化组合删除部 113,在重复组合删除结果的条目中,去除包含在其他条目中示出的用户的组合中、作为可以备份的用户的组合而没有意义的组合,从而生成使用用户信息来记载的基于用户的访问结构。

[0160] 一般访问结构秘密分散部 114 是用于根据基于用户的访问结构,对秘密密钥 205 进行秘密分散的功能。

[0161] 即,一般访问结构秘密分散部 114 分割作为秘密信息的秘密密钥 205,而生成秘密密钥片断(分割秘密信息)。

[0162] 一般访问结构秘密分散部 114 是秘密信息分割部的例子。

[0163] 接下来,根据图 18,对本实施方式的秘密密钥备份装置 101 的动作进行说明。

[0164] 首先在 S1801 中,备份参加用户一览取得部 102 取得示出了参加到系统或者应用程序所管理的备份中的用户的一览、和由该用户进行有效化的角色的一览的备份参加用户一览 201。

[0165] 图 2 示出该备份参加用户一览 201 的结构。

[0166] 备份参加用户一览 201 列举出在备份中列出的参加用户名 2011、和各参加用户进行了激活化的有效化角色 2012 的对。

[0167] 在图 3 所示的例子中,能够示出使角色 RoleC 激活化的用户 UserC 参加、或者使角色 RoleA 和角色 RoleB 同时有效化的用户 UserA 参加的情况等。

[0168] 接下来,在 S1802 中,基于角色的访问结构取得部 103 从系统或者应用程序所管理的安全策略中,取得作为可以复原秘密密钥 205 的角色(指定角色)的组合的基于角色的访问结构 202。

[0169] 图 4 示出该基于角色的访问结构 202 的结构。

[0170] 基于角色的访问结构 202 由表示条目的编号的组合的编号、和使用角色和 AND/OR 等算子来记述的可复原组合构成。

[0171] 在图 5 所示的例子中,在组合编号 No1 中是指定成在角色 RoleA 的用户存在 2 名的情况下,可以复原秘密密钥 205 的例子,在组合编号 No2 中是指定成通过角色 RoleA 的用户必需被列出、进而角色 RoleB 的用户、角色 RoleC 的用户或者角色 RoleD 的用户中的某 2 名被列出,可以复原秘密密钥 205 的例子。

[0172] 接下来,在 S1803 中,角色层次信息取得部 104 从系统或者应用程序所管理的安全策略中,取得在由 RBAC 规定的角色之间关联起来的角色层次信息 203。

[0173] 图 6 示出该角色层次信息 203 的结构。

[0174] 角色层次信息 203 由作为定义层次结构的对象的角色、和表示继承哪个角色的继承源角色构成。

[0175] 角色意味着还可以承担继承源角色的职责。

[0176] 例如,如图 7 所示,记载为角色是 RoleD、继承源角色是 RoleA 的情况下,意味着属于角色 RoleD 中的用户还可以承担角色 RoleA 的职责。

[0177] 即, RoleD 是上位角色, RoleA 是下位角色, RoleD 包含 RoleA。

[0178] 接下来, 在 S1804 中, 同时有效化禁止角色组合取得部 105 从系统或者应用程序所管理的安全策略中, 取得表示用户不得同时进行有效化的角色的组合的同时有效化禁止角色组合 204。

[0179] 图 8 示出该同时有效化禁止角色组合 204 的结构。

[0180] 同时有效化禁止角色组合 204 由表示条目的编号的禁止编号、以及使用角色和不得同时进行有效化的角色数来记述的禁止角色组合构成。

[0181] 在图 9 所示的例子中, 在禁止编号 No1 中是指定为角色 RoleA、角色 RoleB、和角色 RoleC 中的 2 个以上的角色不得同时进行有效化的例子, 在禁止编号 No2 中是指定为角色 RoleA、角色 RoleC 和角色 RoleD 中的直至 2 个角色可以同时进行有效化, 但 3 个以上不得同时进行有效化的例子。

[0182] 接下来, 在 S1805 中, 备份对象秘密密钥取得部 106 取得用户想要进行备份的秘密密钥 205, 而作为系统或者应用程序所管理的秘密信息。

[0183] 该秘密密钥 205 可以是例如公知的 RSA (Rivest-Shamir-Adleman) (注册商标) 密码的秘密密钥, 或者也可以是 AES (Advanced Encryption Standard, 高级加密标准) 密码的密钥。

[0184] 接下来, 在 S1806 中, 所有组合生成部 107 对基于角色的访问结构 202 中包含的指定角色, 应用备份参加用户一览 201 中记载的用户和有效化角色, 从而生成作为有可能可以复原秘密密钥 205 的用户的所有组合的、所有组合抽出结果。

[0185] 此时, 如果对角色定义了层次结构, 则还考虑该层次结构来应用用户和有效化角色。另外, 用括号还一并记载由本来的基于角色的访问结构 202 指定的指定角色。

[0186] 图 10 示出该所有组合抽出结果 (组合抽出信息) 的结构。

[0187] 所有组合抽出结果由表示条目的编号的组合的编号; 和列举了用户、有效化角色、和指定角色的可复原组合构成。

[0188] 图 11 所示的例子是根据图 3 的例子、图 5 的例子、图 7 的例子制作出的所有组合抽出结果。例如, 在图 5 的组合编号 No1 中, 指定了指定角色 RoleA 和指定角色 RoleA, 在图 3 的例子中, 参加用户名 UserA 和参加用户名 UserD 具有有效化角色 RoleA, 所以生成图 11 的组合编号 No1、No2、No3、No4 这 4 个条目的组合。

[0189] 另外, UserA@RoleA (RoleA) 是指, 可以行使角色 RoleA 的权限的用户 UserA 被设置成本来的基于角色的访问结构 202 的指定角色 RoleA。

[0190] 此处, 在组合编号 No1、No4 中, 对指定角色 RoleA 重复设置了同一用户, 但在接下来的步骤中删除重复, 所以在该步骤中不必介意重复, 而列举出所有组合。

[0191] 对于图 11 的组合编号 No5 ~ No12, 也同样地生成。另外, 角色 RoleD/RoleE/RoleF 由于继承了角色 RoleA, 所以也可以作为属于角色 RoleA 中的用户进行处理, 但由于不存在使角色 RoleD/RoleE/RoleF 有效化的用户, 所以不会对所有组合抽出结果造成影响。

[0192] 另一方面, 如果如图 19 所示 UserA 使 RoleD 有效化, 则对于 UserA, 针对图 5 的组合 No1, 作为与 RoleA 符合而抽出, 针对图 5 的组合 No2, 作为与 RoleA、RoleB 以及 RoleD 符合而抽出。

[0193] 接下来, 在 S1807 中, 同一用户・角色删除部 108 在所有组合抽出结果的各项目中

重复出现了属于某有效化角色或者指定角色中的用户的情况下,删除该条目,而生成同一用户・角色删除结果。

[0194] 另外,在对角色定义了层次结构的情况下,将处于父子关系的有效化角色、指定角色也视为同一角色而删除重复。

[0195] 同一用户・角色删除结果的结构与图 8 相同,仅保存的值不同。

[0196] 图 12 是根据图 11 删除了包含同一用户・角色的条目的结果,图 11 的组合编号 No1 重复利用了 UserA@RoleA(RoleA),并且组合编号 No4 重复利用了 UserD@RoleA(RoleA),所以对其进行检测并删除。在本例子中,有效化角色和指定角色两方都相同,但也可以在将某一个可以视为相同的情况下删除。

[0197] 另外,如果如图 19 所示 UserA 使 RoleD 有效化,则根据继承关系,对于图 5 的组合 No1,在所有组合抽出结果中包含 2 个“UserA@RoleD(RoleA)+UserA@RoleD(RoleA)”这样的条目,但由同一用户・角色删除部 108,删除该 2 个条目。

[0198] 接下来,在 S1808 中,同时有效化禁止角色删除部 109,在同一用户・角色删除结果中,某用户使多个由图 9 的同时有效化禁止角色组合 204 指定的组合的角色有效化的情况下,删除该条目,而生成同时有效化禁止角色删除结果。

[0199] 另外,在对角色定义了层次结构的情况下,针对处于父子关系的角色,也与同时有效化禁止角色的条件进行比较,如果有被禁止的组合,则删除该条目。

[0200] 同时有效化禁止角色删除结果的结构与图 10 相同,仅保存的值不同。图 13 是根据图 12 删除利用了同时有效化禁止角色的条目而得到的结果,对于图 12 的组合编号 No5 和 No6,用户 UserA 使角色 RoleA 和角色 RoleB 同时有效化,但在图 9 的同时有效化禁止角色组合 204 的禁止编号 No1 中,角色 RoleA 和角色 RoleB 的同时有效化被禁止,所以对其进行检测而删除。

[0201] 另外,如果如图 19 所示 UserA 使 RoleD 有效化,则根据继承关系,对于图 5 的组合 No2,在所有组合抽出结果中包含“UserA@RoleD(RoleA)+UserA@RoleB(RoleB)+UserB@RoleC(RoleC)”、“UserA@RoleD(RoleA)+UserA@RoleB(RoleB)+UserA@RoleD(RoleD)”这样的条目,但在图 9 的同时有效化禁止角色组合 204 的禁止编号 No1 中,角色 RoleA 和角色 RoleB 的同时有效化被禁止,所以由同时有效化禁止角色删除部 109 删除这些条目。

[0202] 接下来,在 S1809 中,角色信息删除部 110,虽然在同时有效化禁止角色删除结果中还一并记载有用户所属的有效化角色(@ 之后的角色)和指定角色(括号内的角色),但删除该其角色信息,来生成角色信息删除结果。

[0203] 角色信息删除结果的结构与图 10 相同,不同之处在于,作为可复原组合仅使用用户信息进行了指定。

[0204] 图 14 是根据图 13 删除了角色信息的结果,以往是使用用户名/角色的对,但是删除了角色信息的结果,仅通过用户名指定了可复原组合。

[0205] 接下来,在 S1810 中,重复用户信息共用化部 111 在角色信息删除结果中的各条目中出现了同一用户的情况下,将其作为重复而去除,从而生成重复用户信息共用化结果。

[0206] 重复用户信息共用化结果的结构与图 10 相同,作为可复原组合仅使用用户信息来指定这一点不同。

[0207] 图 15 是根据图 14 去除重复出现的用户而得到的结果,在图 14 的组合编号 No7 和

No11 中在可复原组合中重复出现了用户 UserB,所以删除该重复,削减成用户 UserB 仅出现 1 次。

[0208] 接下来,在 S1811 中,重复组合删除部 112,在重复用户信息共用化结果中,去除仅用户信息的记载顺序不同而表示相同的用户的组合的重复组合,从而生成重复组合删除结果。

[0209] 重复组合删除结果的结构与图 10 相同,作为可复原组合仅使用用户信息来进行了指定这一点不同。

[0210] 图 16 是根据图 15 删除用户的记载顺序不同的组合而得到的结果,在图 15 的组合编号 No2 和 No3 中,仅用户 UserA 和用户 UserD 的记载顺序不同,所以去除该重复。

[0211] 接下来,在 S1812 中,无效化组合删除部 113,在重复组合删除结果的条目中,去除包含在其他条目中示出的用户的组合中、而作为可以备份的用户的组合没有意义的组合,从而生成使用用户信息来记载的基于用户的访问结构。

[0212] 基于用户的访问结构的结构与图 10 相同,作为可复原组合仅使用用户信息来进行指定这一点不同。

[0213] 图 17 是根据图 16 删除包含在其他条目中的条目而得到的结果,由于图 16 的组合编号 No8 是如果在组合编号 No7 中可以复原密钥,则自动成立,所以视为包含在 No7 中而删除。

[0214] 同样地,组合编号 No9 和组合编号 No10 包含在组合编号 No2 中,组合编号 No12 包含在组合编号 No11 中,所以删除。

[0215] 最后,在 S1813 中,一般访问结构秘密分散部 114 根据基于用户的访问结构,对秘密密钥 205 进行秘密分散。

[0216] 通过将图 17 所示的用用户信息记载的访问结构作为输入来提供,可以按照以往技术来进行秘密分散,所以使用这些技术根据秘密密钥 205 来生成秘密密钥片断。

[0217] 然后,对在图 2 中接收到的参加用户分发该秘密密钥片断。当然,即使是图 2 中记载的用户,对图 17 的可复原组合中没有出现的用户,也可存在没有所分发的秘密密钥片断的情况。

[0218] 另外,在分发中,例如,通过 LAN(Local Area Network,局域网)等网络、与装置连接的 IC 卡或 USB 存储器等连接端子、PCI 总线等扩展卡连接总线等,对成为对象的用户配送秘密密钥片断。

[0219] 另外,在所有组合生成部 107 中生成的所有组合抽出结果中,与用户信息一起一并记载了在基于角色的访问结构 202 中记载的指定角色(括号内的角色)、和由用户进行有效化的有效化角色(@ 之后的角色)。

[0220] 在想要简化算法的情况下,也可以仅记载指定角色、有效化角色中的某一个。特别在不支持角色层次结构的情况下,可以削减处理数据量,所以是有效的。

[0221] 另外,在基于角色的访问结构是单纯的结构的情况下,也可以不一并记载指定角色、有效化角色,而仅列举出用户信息。

[0222] 另外,在本方式中假设在角色中存在层次结构、同时有效化禁止角色,但根据 RBAC 的软件,还有不支持角色层次结构、同时有效化禁止角色的软件。

[0223] 在该情况下,也可以省略所有组合生成部 107、同一用户・角色删除部 108、同时

有效化禁止角色删除部 109 中的使用了角色层次结构的处理、同时有效化禁止角色删除部 109 中的检测同时有效化禁止角色的处理。

[0224] 另外,在本方式中,在确定了参加到备份中的用户是谁之后,对该用户生成所有组合抽出结果。

[0225] 代替地,也可以设为备份参加用户一览取得部 102 取得属于角色中的所有用户信息,不论是否在备份中列出,都通过所有组合生成部 107 使用所有用户信息来生成所有组合。

[0226] 另外,对于同一用户・角色删除部 108 和同时有效化禁止角色删除部 109,其处理顺序不分先后,所以也可以对图 1 中记载的次序进行交换。

[0227] 关于重复用户信息共用化部 111、重复组合删除部 112、无效化组合删除部 113,其处理顺序也不分先后,所以只要是在从所有组合生成部 107 到一般访问结构秘密分散部 114 之间,则也可以在任意部分中实施处理。

[0228] 对于同时有效化禁止角色组合取得部 105,只要是在同时有效化禁止角色删除部 109 的处理之前,则也可以在任意部分中实施。

[0229] 对于备份对象秘密密钥取得部 106,只要是在一般访问结构秘密分散部 114 的处理实施前,则也可以在任意部分中实施。

[0230] 另外,在本实施方式中,根据由用户进行有效化的角色信息来进行了处理,但也可以加上系统代替用户而自动地设为有效的角色信息来进行处理。另外,也可以使用管理者对用户分配的角色、即对用户登记的角色的信息来进行处理。

[0231] 如上所述,在使用角色来指定了访问结构的情况下,使用作为参加到秘密密钥备份中的用户、和该用户进行激活化的角色的一览的备份参加用户一览 201 的信息,生成使用用户信息来指定的访问结构,所以可以使用仅支持使用用户信息记载的基于用户的访问结构的以往的秘密分散技术来进行秘密密钥的备份。

[0232] 另外,从使处理步骤明确化的观点出发,将步骤 S1806、步骤 S1807、步骤 S1808 分别记载为不同的步骤。但是,从存储器使用量削减、处理速度提高等观点来看,也可以同时执行所述 3 个步骤。即,也可以在生成所有组合抽出结果的过程 S1806 中,不生成同一用户・角色重复的条目,进而,也不生成包括同时有效化禁止角色的条目。在该情况下,虽然所有组合抽出结果是成为非常大的表,但由于可以不生成它而直接生成同时有效化禁止角色删除结果,所以实现存储器使用量的削减、处理速度提高。

[0233] 另外,在步骤 S1806 中生成的所有组合抽出结果、在步骤 S1807 中生成的同一用户・角色删除结果、在步骤 S1808 中生成的同时有效化禁止角色删除结果、在步骤 S1809 中生成的角色信息删除结果、在步骤 S1810 中生成的重复用户信息共用化结果、在步骤 S1811 中生成的重复组合删除结果、在步骤 S1812 中生成的基于用户的访问结构是空的情况下,不存在分割秘密信息的组合,因此设为错误。

[0234] 另外,通过在 RBAC 模型中对角色定义层次结构,可以进行权限的继承,而考虑用户进行激活化的角色的层次结构来生成所有组合抽出结果,所以即使在利用了角色层次结构的情况下,也可以正确地解释基于角色的访问结构 202 来生成基于用户的访问结构,对秘密密钥进行秘密分散而生成秘密密钥片断。

[0235] 另外,由于选择并利用在备份中列出的用户信息,所以可以削减基于用户的访问

结构的复杂度,与对所登记的所有用户分发秘密密钥片断的情况相比,可以削减秘密密钥片断的生成处理、片断数。

[0236] 另外,在同一用户・角色删除部 108 中,对属于某有效化角色或者指定角色中的用户被重复计数的情形进行检测,所以可以消除一个用户被计数为多个用户而得到比设想更多的秘密密钥片断的危险。

[0237] 另外,在同时有效化禁止角色删除部 109 中,在秘密密钥备份时进行同时有效化禁止角色的利用检查,对禁止角色的组合进行检测・删除,所以可以支持由 NIST RBAC 模型定义的 Dynamic SoD 策略。

[0238] 另外,在角色信息删除部 110、重复用户信息共用化部 111、重复组合删除部 112、无效化组合删除部中,抽出删除角色信息而仅通过用户信息指定的访问结构,进行重复、包含关系的检查来删除不需要的条目,所以可以生成基于用户的访问结构,可以使用具有作为以往技术的一般访问结构的秘密分散方式根据秘密密钥来生成秘密密钥片断。

[0239] (实施方式 2)

[0240] 实施方式 1 是将作为可以复原秘密密钥的角色的组合的、基于角色的访问结构作为输入而接收到的情况下的秘密密钥备份方式。

[0241] 但是,在 RBAC 中使用访问控制策略信息(以下,还简称为访问控制策略)来管理访问权限,所以系统管理者必须无矛盾地维护访问控制策略和基于角色的访问结构这 2 个。

[0242] 因此,在本实施方式 2 中,说明如下技术:在使用 RBAC 时,根据记述了对管理者、一般用户等操作者许可的操作的访问控制策略,来自动地生成基于角色的访问结构,从而不需要基于角色的访问结构的管理。

[0243] 图 21 是本实施方式的秘密密钥备份系统 3000 的功能结构图。

[0244] 基于角色的访问结构生成装置 2101 是用于根据记述了对管理者、一般用户等操作者许可的操作的访问控制策略信息,自动地生成基于角色的访问结构的装置。作为向实施方式 1 中示出的秘密密钥备份装置 101 的追加功能而利用。

[0245] 在图 21 中,秘密密钥 205、角色层次信息 203、备份对象秘密密钥取得部 106、角色层次信息取得部 104 与实施方式 1 相同,所以省略说明。

[0246] 访问控制策略 2102 是记述了对管理者、一般用户等操作者许可的操作(以下,称为访问权限)的信息,是与本装置一起使用的 RBAC 系统中利用的信息。

[0247] 访问权限一般如图 23、图 24 所示,由表示“对谁”的许可角色名(将许可角色还称为执行者角色)、表示“把什么”的许可操作对象、以及表示“怎么做”的许可操作内容来构成。

[0248] 进而,选择性地指定了多个表示所许可的“条件”的许可者。

[0249] 该许可者并非用户名而是通过角色(许可者角色)指定,有时在不需要许可的情况下不指定。另外,此处记载的许可者角色的数量 N 是可变的,所以针对每个系统是不同的值。通过列举出多个它们的访问权限,而构成了访问控制策略 2102。

[0250] 这样,访问控制策略 2102 是将针对限制了访问的秘密密钥(秘密信息)的访问被许可的许可角色、和对许可角色许可针对秘密密钥的访问的 1 个以上的许可者角色的组合示出多个的信息。

[0251] 备份执行用户信息 2103 是想要执行备份处理的用户的执行用户名、和该用户进行有效化的有效化角色的一览。

[0252] 如图 25 所示,是由可以确定用户个人的执行用户名、和作为用户进行了有效化的角色的有效化角色 1 ~ 有效化角色 M 构成的信息。此处记载的有效化角色的数量 M 是用户进行了有效化的角色的数量,所以是根据进行备份时的状况而变化的值。

[0253] 这样,备份执行用户信息 2103 是表示执行针对秘密密钥的访问的执行用户的有效化角色(执行用户角色)的信息,是执行用户信息的例子。

[0254] 备份许可用户一览 2104 是将许可了备份执行用户进行备份的用户的用户名、和在进行了许可时有效化的有效化角色的组合作为一览表的信息。

[0255] 如图 22 所示,是将许可了备份的用户的许可用户名、和在许可用户进行了许可时有效化的有效化角色的对作为一览表的结构。

[0256] 这样,备份许可用户一览 2104 是表示对执行用户许可了针对秘密密钥的访问的许可用户的有效化角色(许可用户角色)的信息,是许可用户信息的例子。

[0257] 访问控制策略取得部 2105 是取得访问控制策略 2102 的功能。

[0258] 访问控制策略取得部 2105 是访问控制策略信息取得部的例子。

[0259] 备份执行用户信息取得部 2106 是取得备份执行用户信息 2103 的功能。

[0260] 备份执行用户信息取得部 2106 是执行用户信息取得部的例子。

[0261] 备份许可用户一览取得部 2107 是取得备份许可用户一览 2104 的功能。

[0262] 备份许可用户一览取得部 2107 是许可用户信息取得部的例子。

[0263] 备份权限抽出部 2108 是用于在访问控制策略 2102 中记载的各种访问权限中,仅抽出记载了与备份相关的访问权限的信息的功能。

[0264] 为了进行抽出,从备份对象秘密密钥取得部 106 中收领秘密密钥。然后,仅抽出访问控制策略 2102 的、许可操作对象表示所收领的秘密密钥、并且许可操作内容表示备份操作的信息。将通过该抽出得到的结果以下称为“访问权限一览(备份权限抽出结果)”。

[0265] 有效访问权限抽出部 2109 是根据从所述备份权限抽出部 2108 接收的访问权限一览(备份权限抽出结果),考虑备份执行用户信息 2103、备份许可用户一览 2104、角色层次信息 203,而抽出可以用作用于生成基于角色的访问结构的源信息(original information)的访问权限的功能。将通过该抽出得到的结果以下称为“访问权限一览(有效访问权限抽出结果)”。

[0266] 基于角色的访问结构生成部 2110 是用于根据由有效访问权限抽出部 2109 抽出的访问权限一览(有效访问权限抽出结果),生成基于角色的访问结构的功能。所制作的基于角色的访问结构与实施方式 1 所示的结构相同。

[0267] 备份部 101 相当于实施方式 1 中示出的秘密密钥备份装置 101,由以下部分构成:备份参加用户一览取得部、基于角色的访问结构取得部、角色层次信息取得部、同时有效化禁止角色组合取得部、备份对象秘密密钥取得部、所有组合生成部、同一用户·角色删除部、同时有效化禁止角色删除部、角色信息删除部、重复用户信息共用化部、重复组合删除部、无效化组合删除部、一般访问结构秘密分散部。

[0268] 由于与实施方式 1 相同,所以省略详细说明。

[0269] 接下来,根据图 26,对本实施方式的秘密密钥备份系统 3000 的动作进行说明。

[0270] 首先在 S2601 中,访问控制策略取得部 2105 从系统或者应用程序所管理的安全策略中,取得访问控制策略 2102。

[0271] 图 23 示出该访问控制策略 2102 的结构。

[0272] 访问控制策略 2102 是列举出由许可角色名、许可操作内容、许可操作对象、许可者 1 至许可者 N 构成的访问权限的一览表。

[0273] 许可角色名是指定将访问权限分配给哪个角色的信息。

[0274] 许可操作内容是表示许可什么样的操作的信息。

[0275] 许可操作对象是表示定义针对秘密密钥、日志信息等什么样的信息的访问权限的信息。

[0276] 许可者 1 至许可者 N 是表示该访问权限在存在哪个角色的许可时将访问权限视为有效的信息。

[0277] 在图 24 所示的例子的第 1 行中,使由许可角色名指定的 RoleA 有效化的用户,拥有对由许可操作对象指定的秘密密钥 1 实施许可操作内容中示出的备份的访问权限,是限于如由许可者 1 指定那样属于 RoleA 中的用户提供了进行备份的许可的情况(在如第 2 行那样存在多个许可者角色的情况下,限于属于所有许可者角色中的用户提供了许可的情况)这样的访问权限。

[0278] 这样的访问权限成为一览表的形式而构成访问控制策略 2102。

[0279] 接下来,在 S2602 中,备份执行用户信息取得部 2106 取得与想要执行系统或者应用程序所管理的备份处理的用户相关的备份执行用户信息 2103。

[0280] 图 25 示出该备份执行用户信息 2103 的结构。

[0281] 备份执行用户信息 2103 由执行用户名和有效化角色 1 至有效化角色 M 构成。

[0282] 执行用户名表示想要执行备份处理的用户的用户名。另外,有效化角色 1 至有效化角色 M 是用户进行有效化的角色的一览。

[0283] 接下来,在 S2603 中,备份许可用户一览取得部 2107 从系统或者应用程序所管理的安全策略中,取得对在 S2602 中取得的备份执行用户信息 2103 中包含的用户进行备份这样的操作,许可其备份处理的许可者的角色的一览即备份许可用户一览 2104。

[0284] 针对每个执行用户、操作对象(秘密密钥 1 等)、操作内容(备份等),存在备份许可用户一览 2104。

[0285] 图 22 示出备份许可用户一览 2104 的结构。

[0286] 备份许可用户一览 2104 是列举出许可用户名和有效化角色的对的一览表。

[0287] 许可用户名是对备份执行用户进行备份这样的操作,许可了其备份处理的许可者的用户名。

[0288] 有效化角色是在许可用户进行了备份的许可时有效化的角色。

[0289] 接下来,在 S2604 中,角色层次信息取得部 104 从系统或者应用程序所管理的安全策略中,取得在由 RBAC 规定的角色之间关联起来的角色层次信息 203。

[0290] 该角色层次信息 203 的结构与实施方式 1 中示出的角色层次信息 203 相同,所以省略说明。

[0291] 接下来,在 S2605 中,备份对象秘密密钥取得部 106 从系统或者应用程序所管理的安全策略中,取得用户想要进行备份的秘密密钥。

[0292] 如实施方式 1 所示,该秘密密钥可以是例如公知的 RSA(注册商标)密码的秘密密钥,或者也可以是 AES 密码的共用密钥。

[0293] 接下来,在 S2606 中,备份权限抽出部 2108,在 S2601 中取得的访问控制策略 2102 中记载的各种访问权限中,仅抽出与备份相关的访问权限。

[0294] 在抽出中,仅抽出访问控制策略 2102 的、许可操作对象表示在 S2605 中取得的秘密密钥、并且许可操作内容表示备份操作的信息。

[0295] 该抽出是访问权限一览(备份权限抽出结果),结构与访问控制策略 2102 相同。

[0296] 接下来,在 S2607 中,有效访问权限抽出部 2109 从在 S2606 中生成的访问权限一览(备份权限抽出结果)中,考虑备份执行用户信息 2103、备份许可用户一览 2104、角色层次信息 203,抽出可以用作用于生成基于角色的访问结构的源信息的访问权限一览(有效访问权限抽出结果)。

[0297] 示出两个该抽出算法的主要的例子。

[0298] 最初的抽出方式例 1 是进行严密的检查的方式。

[0299] 首先,从备份执行用户信息 2103 中取得有效化角色 1~有效化角色 M,抽出与在 S2606 中生成的访问权限一览(备份权限抽出结果)的许可角色名一致的角色。

[0300] 此时,考虑角色层次信息 203,还包括访问权限一览(备份权限抽出结果)的许可角色名与用户进行有效化的有效化角色 1~有效化角色 M 的下位角色相应的情况,视为一致而抽出。

[0301] 进而,确认许可者 1~许可者 N 中记载的所有角色是否记载于备份许可用户一览 2104 的有效化角色中的某一个中,而仅在包含时抽出。

[0302] 此时,考虑角色层次信息 203,还包括许可者 1~许可者 N 中记载的角色与备份许可用户进行有效化的有效化角色的下位角色相应的情况,视为一致而抽出。

[0303] 另外,在许可者 1 至许可者 N 中,关于没有指定角色的许可者无需进行比较处理,而仅针对指定的许可者进行比较处理即可。

[0304] 通过以上操作,生成为了生成基于角色的访问结构而所需的访问权限一览(有效访问权限抽出结果)。

[0305] 抽出方式例 2 是使比较条件缓和的方式,是不区分执行用户和许可用户而进行抽出的方式。

[0306] 具体而言,是如下方式:仅抽出在 S2606 中生成的访问权限一览(备份权限抽出结果)的许可角色名和许可者 1 至许可者 N 的全部包含在备份执行用户信息 2103 中记载的有效化角色 1~有效化角色 M、或者备份许可用户一览 2104 的有效化角色中的某一方中的访问权限。

[0307] 因此,许可角色名也可以包含在备份许可用户一览 2104 的有效化角色中的某一个中,许可者 1 至许可者 N 的全部也可以包含在备份执行用户信息 2103 中记载的有效化角色 1~有效化角色 M 中。

[0308] 此时,考虑角色层次信息 203,在许可角色名和许可者 1~许可者 N 中记载的角色的上位角色与备份执行用户信息 2103 中记载的有效化角色 1~有效化角色 M、或者、备份许可用户一览 2104 的有效化角色一致的情况下,也抽出。

[0309] 另外,在从许可者 1 至许可者 N 中,关于没有指定角色的许可者,无需进行比较处

理,而仅针对指定的许可者进行比较处理即可。

[0310] 通过以上操作,生成为了生成基于角色的访问结构而所需的访问权限一览(有效访问权限抽出结果)。

[0311] 接下来,在 S2608 中,基于角色的访问结构生成部 2110 根据在 S2607 中生成的访问权限一览(有效访问权限抽出结果),生成基于角色的访问结构。

[0312] 具体而言,从访问权限一览(有效访问权限抽出结果)中取出一个访问权限。

[0313] 将该访问权限中记载的许可角色名和许可者 1 至许可者 N 视为可以复原秘密密钥的角色的组合。

[0314] 即,成为构成图 4 中所示的基于角色的访问结构的表中的 1 行的要素。

[0315] 其中,在存在 {RoleB、RoleC}、{RoleC、RoleD}、{RoleB、RoleD} 这样的组合的情况下,如果如“2of {RoleB、RoleC、RoleD}”那样省略记载,则还可以削减数据量。

[0316] 对访问权限一览(有效访问权限抽出结果)中包含的所有访问权限进行同样的变换而得到的结构成为基于角色的访问结构。

[0317] 最后,在 S2609 中,备份部 101 通过实施方式 1 中示出的方法,除了在 S2608 中生成的基于角色的访问结构以外,还将系统或者应用程序所管理的备份参加用户一览、角色层次信息、同时有效化禁止角色组合、秘密密钥作为输入而接收,生成秘密密钥片断。

[0318] 另外,在图 23 中示出了访问控制策略 2102 的结构,但访问控制策略 2102 的结构根据系统而各种各样。

[0319] 因此,还考虑省略了许可操作内容、许可操作对象的情形。

[0320] 在该情况下,也可以在 S2606 中省略许可操作内容、许可操作对象的比较。

[0321] 另外,同样地,在不存在许可者 1 至许可者 N 的要素的访问控制策略 2102 的情况下,设为在 S2607 和 S2608 中没有指定许可者来进行处理即可。

[0322] 另外,在图 25 中示出的备份执行用户信息 2103 中包括执行用户名,这是因为在实际系统中将执行用户名和有效化角色 1 至有效化角色 M 关联起来管理的情况较多,所以如此记载。

[0323] 但是,由于在本方式的处理中不需要执行用户名,所以也可以从备份执行用户信息 2103 中删除。

[0324] 另外,在图 22 中示出的备份许可用户一览 2104 中,使用了将许可用户名和有效化角色的组设为表的一览。但是,由于在本方式的处理中不需要许可用户名,所以也可以是仅由有效化角色构成的备份许可用户一览 2104。

[0325] 另外,在图 22 中示出的备份许可用户一览 2104 是将许可用户名和有效化角色的组设为表的一览。如果同一许可用户根据多个角色提供了许可的情况下,通过如下那样的方法来列举即可。

[0326] 即,(1)在有效化角色中列举多个角色信息(在 1 个记录中列举多个角色信息)。(2)作为对有效化角色仅指定 1 个角色的补偿,而列举许可用户名和有效化角色的多个组(对 1 个记录指定 1 个角色,并且设置多个记录)。

[0327] 另外,在图 25 中示出的备份执行用户信息 2103 的有效化角色 1 至有效化角色 N、在图 22 中示出的备份许可用户一览 2104 的有效化角色中,记载了用户明示地进行了有效化的角色信息的情况较多,但也可以记载系统代替用户而自动地设为有效的角色信息。另

外,也可以将管理者对用户分配的角色、即对用户登记的角色信息记载为有效化角色。

[0328] 另外,S2601、S2602、S2603、S2604、S2605 是分别独立的处理,所以无需按照记载的顺序来执行。在 S2606 之前执行 S2601,在 S2607 之前执行 S2602,在 S2607 之前执行 S2603,在 S2607 之前执行 S2604,在 S2606 之前执行 S2605 即可。

[0329] 另外,在 S2605 中,例示了备份对象秘密密钥取得部将 RSA(注册商标)密码的秘密密钥、AES 密码的共用密钥作为输入而接收,但只要所接收的信息是进行备份的信息,则不必就是密码算法的密钥。例如,也可以是机密文档、顾客信息等信息。

[0330] 另外,在 S2606 中,备份权限抽出部 2108 仅实施基于许可操作内容和许可操作对象的缩小,而制作出结构上与访问控制策略 2102 同样的访问权限一览(备份权限抽出结果)。但是,在以后的处理中,不需要许可操作内容和许可操作对象的信息,所以也可以是从访问控制策略 2102 中删除了许可操作内容和许可操作对象的结构。关于访问权限一览(有效访问权限抽出结果)的结构也是同样的。

[0331] 另外,在 S2606 中,备份权限抽出部 2108 在 S2601 中取得的访问控制策略 2102 中记载的各种访问权限中,仅抽出了与备份相关的访问权限。其原因为,示出的是在秘密信息管理装置中对秘密密钥进行备份的情况的例子。如果分别定义了备份和还原的权限,则也可以代替地抽出还原权限来进行处理。另外,在进行秘密分散来取得秘密信息的操作中,考虑到每个系统中称为不同的名称,所以需要通过适合于该系统的操作名来进行检索。

[0332] 另外,在 S2607 中在有效访问权限抽出部 2109 中,根据备份执行用户信息 2103、备份许可用户一览 2104、和角色层次信息 203 抽出了有效的访问权限,但对此也可以还考虑同时有效化禁止角色组合来进行缩小。

[0333] 另外,在本实施方式中,针对在访问权限一览(备份权限抽出结果)中记述的许可角色以及许可者角色,将备份执行用户信息中包含的角色以及备份许可用户一览中包含的角色进行对照,而生成基于角色的访问结构。

[0334] 代替地,也可以根据在访问权限一览(备份权限抽出结果)中记述的许可角色以及许可者角色来生成基于角色的访问结构。

[0335] 例如,也可以根据图 24 的第 1 行的记录来生成 {RoleA,RoleA} 这样的基于角色的访问结构,或者根据第 2 行的记录来生成 {RoleA,RoleB,RoleC} 这样的基于角色的访问结构。

[0336] 另外,在步骤 S2606 中生成的访问权限一览(备份权限抽出结果)、在步骤 S2607 中生成的访问权限一览(有效访问权限抽出结果)、在步骤 S2608 中生成的基于角色的访问结构是空的情况下,不存在分割秘密信息的组合,从而设为错误。

[0337] 如上所述,依据在访问控制策略 2102 中指定的许可备份的访问权限,根据备份执行用户信息 2103、备份许可用户一览 2104、角色层次信息 203 来生成基于角色的访问结构,所以只要仅维护访问控制策略 2102,就可以自动地计算出可以复原秘密密钥的角色的组合,灵活地进行秘密密钥的备份。

[0338] 另外,由于考虑用户进行有效化的角色的层次结构、进行了备份的许可的用户进行有效化的角色的层次结构来生成访问权限一览(有效访问权限抽出结果),所以即使在利用了角色层次结构的情况下,也可以正确且自动地生成基于角色的访问结构,对秘密密钥进行秘密分散而生成秘密密钥片断。

[0339] 另外,由于选择并利用实施了备份的用户、进行了许可的用户的信息,所以可以减少所生成的基于角色的访问结构的复杂度,所以与对在访问控制策略 2102 中登记了备份的访问权限的所有用户分发秘密密钥片断的情况相比,可以削减秘密密钥片断的生成处理、片断数。

[0340] 最后,对实施方式 1、2 所示的秘密密钥备份装置 101 以及基于角色的访问结构生成装置 2101(以下,称为秘密密钥备份装置 101 等)的硬件结构例进行说明。

[0341] 图 20 是示出实施方式 1、2 所示的秘密密钥备份装置 101 等硬件资源的一个例子的图。

[0342] 另外,图 20 的结构仅示出秘密密钥备份装置 101 等硬件结构的一个例子,秘密密钥备份装置 101 等硬件结构不限于图 20 记载的结构,而也可以是其他结构。

[0343] 在图 20 中,秘密密钥备份装置 101 等具备执行程序的 CPU911(Central Processing Unit,还称为中央处理装置、处理装置、运算装置、微处理器、微型计算机、处理器)。

[0344] CPU911 经由总线 912,例如,与 ROM(Read Only Memory)913、RAM(Random Access Memory)914、通信板 (communication board)915、显示装置 901、键盘 902、鼠标 903、磁盘装置 920 连接,对这些硬件设备进行控制。

[0345] 进而,CPU911 也可以与 FDD904(Flexible Disk Drive)、高密度盘装置 905(CDD)、打印机装置 906、扫描仪装置 907 连接。另外,也可以代替磁盘装置 920,而使用光盘装置、存储卡(注册商标)读写装置等存储装置。

[0346] RAM914 是易失性存储器的一个例子。ROM913、FDD904、CDD905、磁盘装置 920 的存储介质是非易失性存储器的一个例子。它们是存储装置的一个例子。

[0347] 通信板 915、键盘 902、鼠标 903、扫描仪装置 907、FDD904 等是输入装置的一个例子。

[0348] 另外,通信板 915、显示装置 901、打印机装置 906 等是输出装置的一个例子。

[0349] 例如,通信板 915 与 LAN(局域网)、因特网、WAN(广域网)等连接。

[0350] 在磁盘装置 920 中,存储了操作系统 921(OS)、视窗系统 (window system)922、程序群 923、文件群 924。

[0351] CPU911 利用操作系统 921、视窗系统 922 来执行程序群 923 的程序。

[0352] 另外,在 RAM914 中,暂时保存了使 CPU911 执行的操作系统 921 的程序、应用程序的程序中的至少一部分。

[0353] 另外,在 RAM914 中,保存了由 CPU911 进行的处理中所需的各种数据。

[0354] 另外,在 ROM913 中,保存了 BIOS(Basic Input Output System,基本输入输出系统)程序,在磁盘装置 920 中,保存了引导程序 (boot program)。

[0355] 在秘密密钥备份装置 101 等起动时,执行 ROM913 的 BIOS 程序以及磁盘装置 920 的引导程序,通过 BIOS 程序以及引导程序,起动操作系统 921。

[0356] 在所述程序群 923 中,存储了执行在实施方式 1、2 的说明中说明为“~部”的功能的程序。由 CPU911 读出并执行程序。

[0357] 在文件群 924 中,也可以包括备份参加用户一览 201、基于角色的访问结构 202、角色层次信息 203、同时有效化禁止角色组合 204、秘密密钥 205、访问控制策略 2102、备份执

行用户信息 2103、备份许可用户一览 2104。

[0358] 另外,所抽出的用户的组合(图 10~图 17)、访问权限一览(备份权限抽出结果)以及访问权限一览(有效访问权限抽出结果)等被存储在 RAM914、磁盘装置 920、未图示的高速缓存存储器、缓冲存储器、寄存器中等。

[0359] 进而,根据秘密密钥 205 生成的秘密密钥片断也被存储在 RAM914、磁盘装置 920、未图示的高速缓存存储器、缓冲存储器、寄存器中等。

[0360] 另外,在文件群 924 中,将表示在实施方式 1、2 的说明中说明为“~的判断”、“~的取得”、“~的抽出”、“~的比较”、“~的删除”、“~的更新”、“~的设定”、“~的登记”、“~的检测”等的处理的结果的信息、数据、信号值、变量值、参数存储为“~文件”、“~数据库”的各项目。

[0361] “~文件”、“~数据库”被存储在盘、存储器等记录介质中。由 CPU911 经由读写电路将存储在盘、存储器等存储介质中的信息、数据、信号值、变量值、参数读出到主存储器、高速缓存存储器中,而用于抽出・检索・参照・比较・运算・计算・处理・编辑・输出・印刷・显示等 CPU 的动作中。

[0362] 在抽出・检索・参照・比较・运算・计算・处理・编辑・输出・印刷・显示的 CPU 的动作的期间,信息、数据、信号值、变量值、参数被暂时存储在主存储器、寄存器、高速缓存存储器、缓冲存储器等中。

[0363] 另外,在实施方式 1、2 中说明的流程图的箭头的部分主要表示数据、信号的输入输出,数据、信号值被记录在 RAM914 的存储器、FDD904 的软盘、CDD905 的高密度盘、磁盘装置 920 的磁盘、其他光盘、迷你盘(mini disk)、DVD 等记录介质中。另外,通过总线 912、信号线、电缆、其他传送介质来在线(online)传送数据、信号。

[0364] 另外,在实施方式 1、2 的说明中说明为“~部”的部分既可以是“~电路”、“~装置”、“~机器”,并且也可以是“~步骤”、“~程序”、“~处理”。即,说明为“~部”的部分也可以通过存储在 ROM913 中的固件来实现。或者,也可以仅通过软件,或者仅通过元件・器件・基板・布线等硬件,或者通过软件和硬件的组合,进而通过与固件的组合来实施。固件和软件作为程序而被存储在磁盘、软盘、光盘、高密度盘、迷你盘、DVD 等记录介质中。由 CPU911 读出并由 CPU911 执行程序。即,程序使计算机作为实施方式 1、2 的“~部”而发挥功能。或者,使计算机执行实施方式 1、2 的“~部”的步骤、方法。

[0365] 这样,实施方式 1、2 所示的秘密密钥备份装置 101 等是具备作为处理装置的 CPU、作为存储装置的存储器、磁盘等、作为输入装置的键盘、鼠标、通信板等、作为输出装置的显示装置、通信板等的计算机,使用这些处理装置、存储装置、输入装置、输出装置来实现如上所述作为“~部”示出的功能。

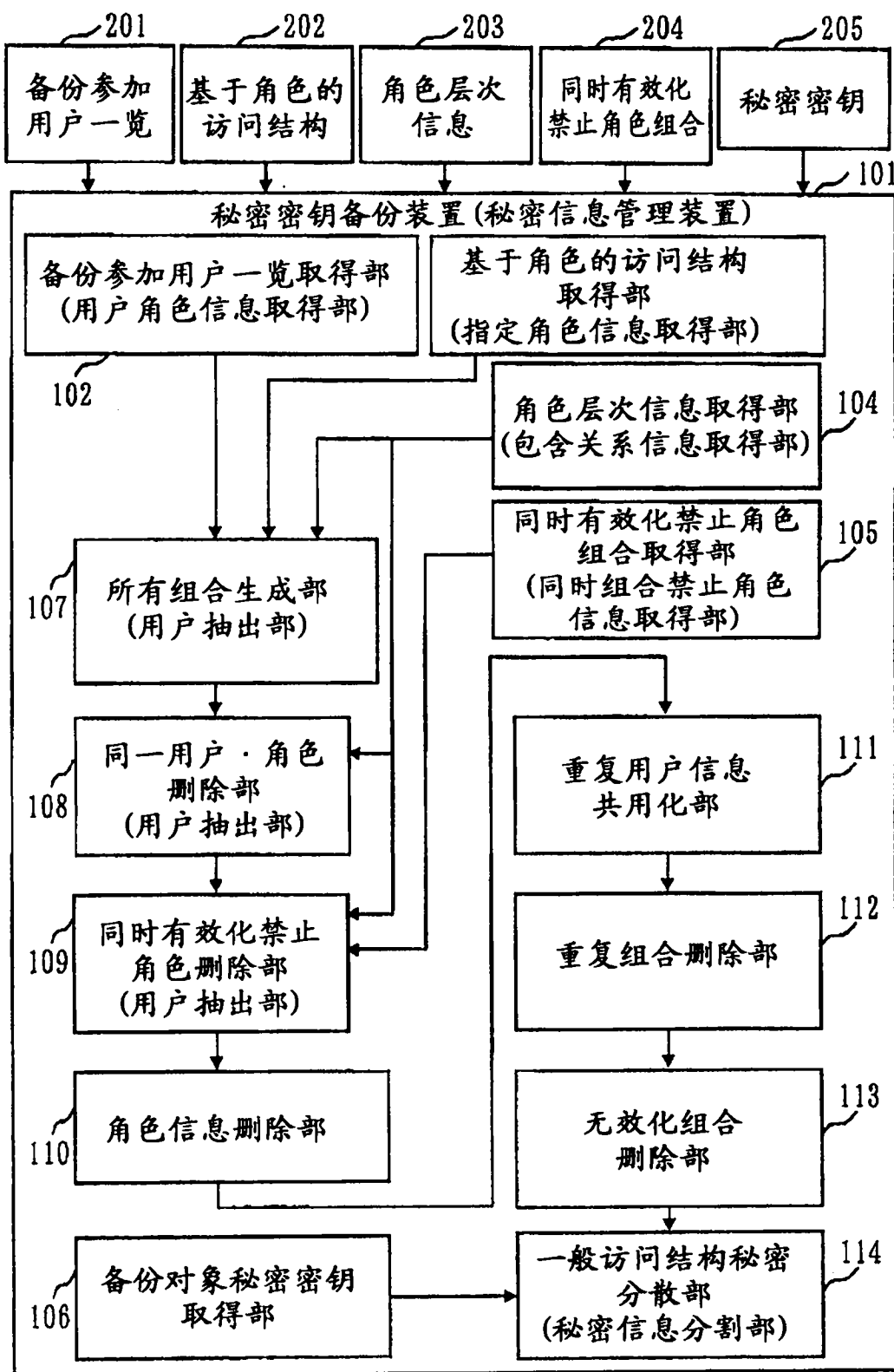


图 1

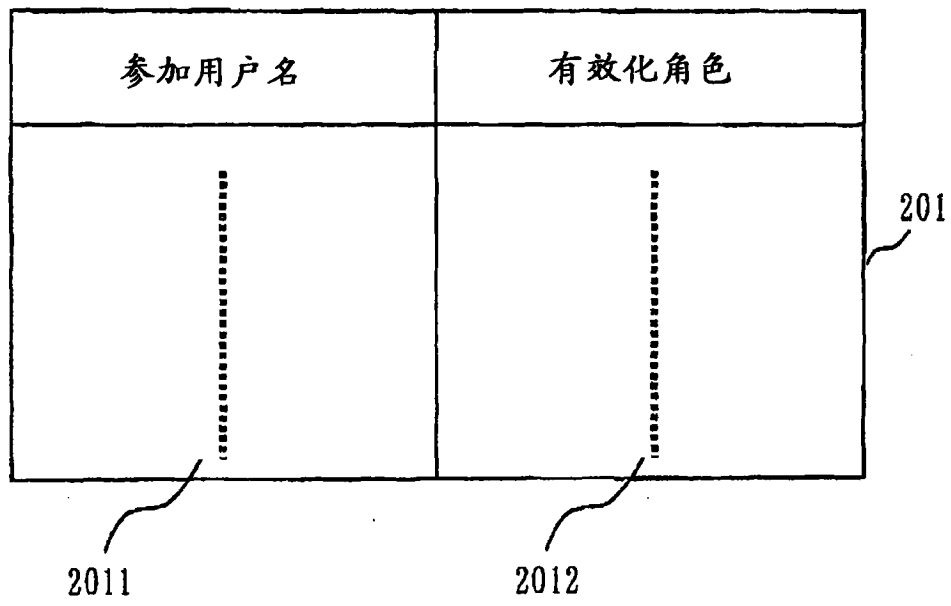


图 2

参加用户名	有效化角色
UserA	RoleA
UserA	RoleB
UserB	RoleB
UserB	RoleC
UserC	RoleC
UserD	RoleA

图 3

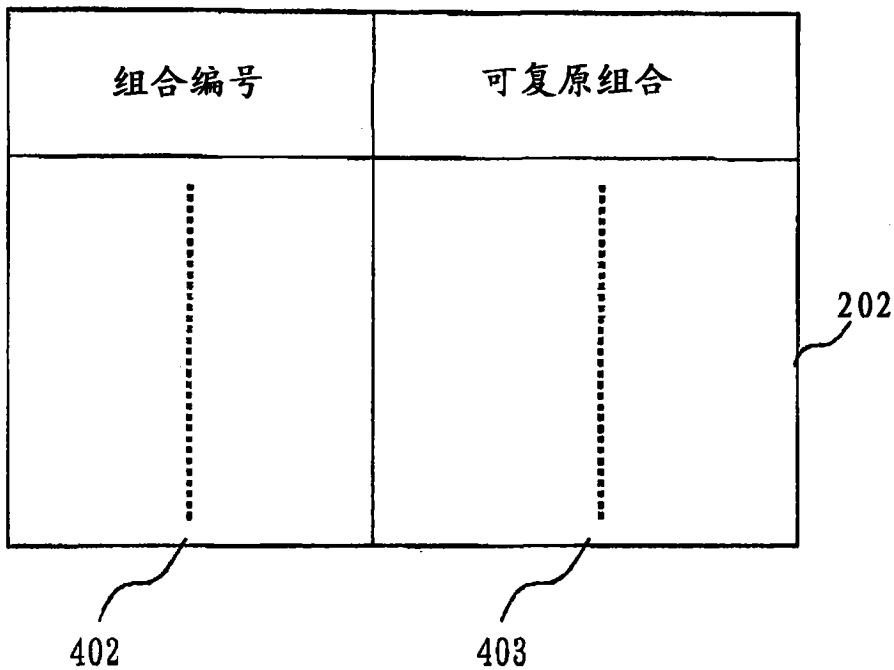


图 4

组合编号	可复原组合
No1	(RoleA, RoleA)
No2	RoleA AND 2 of (RoleB, RoleC, RoleD)

图 5

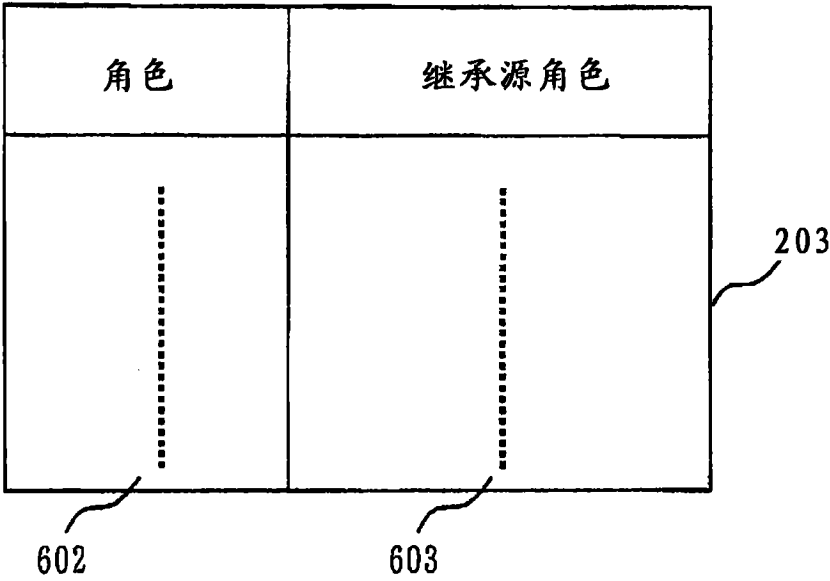


图 6

角色	继承源角色
RoleD	RoleA
RoleE	RoleD
RoleF	RoleE

图 7

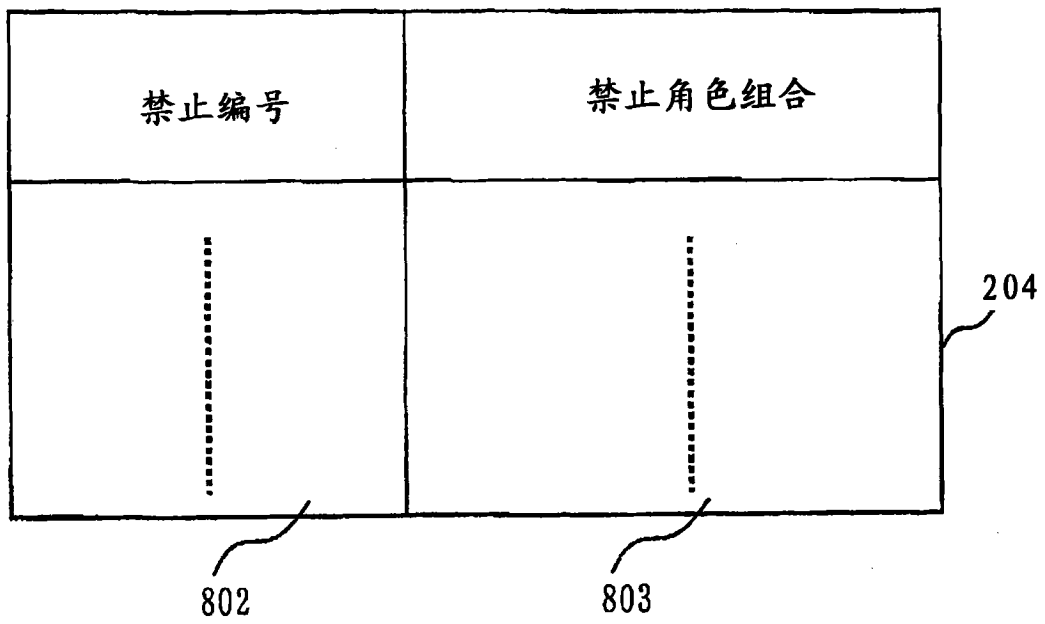


图 8

禁止编号	禁止角色组合
No1	2 of (RoleA, RoleB, RoleC)
No2	3 of (RoleA, RoleC, RoleD)

图 9

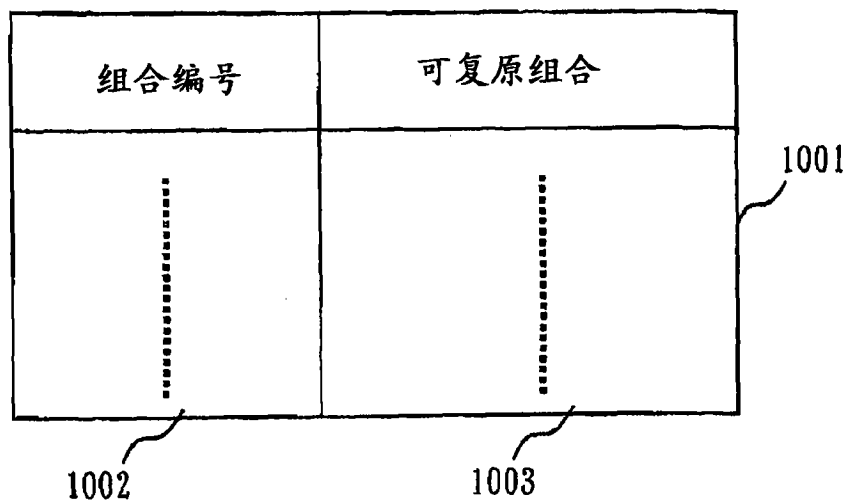


图 10

组合编号	可复原组合
No1	UserA@RoleA (RoleA) +UserA@RoleA (RoleA)
No2	UserA@RoleA (RoleA) +UserD@RoleA (RoleA)
No3	UserD@RoleA (RoleA) +UserA@RoleA (RoleA)
No4	UserD@RoleA (RoleA) +UserD@RoleA (RoleA)
No5	UserA@RoleA (RoleA) +UserA@RoleB (RoleB) +UserB@RoleC (RoleC)
No6	UserA@RoleA (RoleA) +UserA@RoleB (RoleB) +UserC@RoleC (RoleC)
No7	UserA@RoleA (RoleA) +UserB@RoleB (RoleB) +UserB@RoleC (RoleC)
No8	UserA@RoleA (RoleA) +UserB@RoleB (RoleB) +UserC@RoleC (RoleC)
No9	UserD@RoleA (RoleA) +UserA@RoleB (RoleB) +UserB@RoleC (RoleC)
No10	UserD@RoleA (RoleA) +UserA@RoleB (RoleB) +UserC@RoleC (RoleC)
No11	UserD@RoleA (RoleA) +UserB@RoleB (RoleB) +UserB@RoleC (RoleC)
No12	UserD@RoleA (RoleA) +UserB@RoleB (RoleB) +UserC@RoleC (RoleC)

图 11

组合编号	可复原组合
No2	UserA@RoleA (RoleA) +UserD@RoleA (RoleA)
No3	UserD@RoleA (RoleA) +UserA@RoleA (RoleA)
No5	UserA@RoleA (RoleA) +UserA@RoleB (RoleB) +UserB@RoleC (RoleC)
No6	UserA@RoleA (RoleA) +UserA@RoleB (RoleB) +UserC@RoleC (RoleC)
No7	UserA@RoleA (RoleA) +UserB@RoleB (RoleB) +UserB@RoleC (RoleC)
No8	UserA@RoleA (RoleA) +UserB@RoleB (RoleB) +UserC@RoleC (RoleC)
No9	UserD@RoleA (RoleA) +UserA@RoleB (RoleB) +UserB@RoleC (RoleC)
No10	UserD@RoleA (RoleA) +UserA@RoleB (RoleB) +UserC@RoleC (RoleC)
No11	UserD@RoleA (RoleA) +UserB@RoleB (RoleB) +UserB@RoleC (RoleC)
No12	UserD@RoleA (RoleA) +UserB@RoleB (RoleB) +UserC@RoleC (RoleC)

图 12

组合编号	可复原组合
No2	UserA@RoleA (RoleA) +UserD@RoleA (RoleA)
No3	UserD@RoleA (RoleA) +UserA@RoleA (RoleA)
No7	UserA@RoleA (RoleA) +UserB@RoleB (RoleB) +UserB@RoleC (RoleC)
No8	UserA@RoleA (RoleA) +UserB@RoleB (RoleB) +UserC@RoleC (RoleC)
No9	UserD@RoleA (RoleA) +UserA@RoleB (RoleB) +UserB@RoleC (RoleC)
No10	UserD@RoleA (RoleA) +UserA@RoleB (RoleB) +UserC@RoleC (RoleC)
No11	UserD@RoleA (RoleA) +UserB@RoleB (RoleB) +UserB@RoleC (RoleC)
No12	UserD@RoleA (RoleA) +UserB@RoleB (RoleB) +UserC@RoleC (RoleC)

图 13

组合编号	可复原组合
No2	UserA + UserD
No3	UserD + UserA
No7	UserA + UserB + UserB
No8	UserA + UserB + UserC
No9	UserD + UserA + UserB
No10	UserD + UserA + UserC
No11	UserD + UserB + UserB
No12	UserD + UserB + UserC

图 14

组合编号	可复原组合
No2	UserA + UserD
No3	UserD + UserA
No7	UserA + UserB
No8	UserA + UserB + UserC
No9	UserD + UserA + UserB
No10	UserD + UserA + UserC
No11	UserD + UserB
No12	UserD + UserB + UserC

图 15

组合编号	可复原组合
No2	UserA + UserD
No7	UserA + UserB
No8	UserA + UserB + UserC
No9	UserD + UserA + UserB
No10	UserD + UserA + UserC
No11	UserD + UserB
No12	UserD + UserB + UserC

图 16

组合编号	可复原组合
No2	UserA + UserD
No7	UserA + UserB
No11	UserD + UserB

图 17

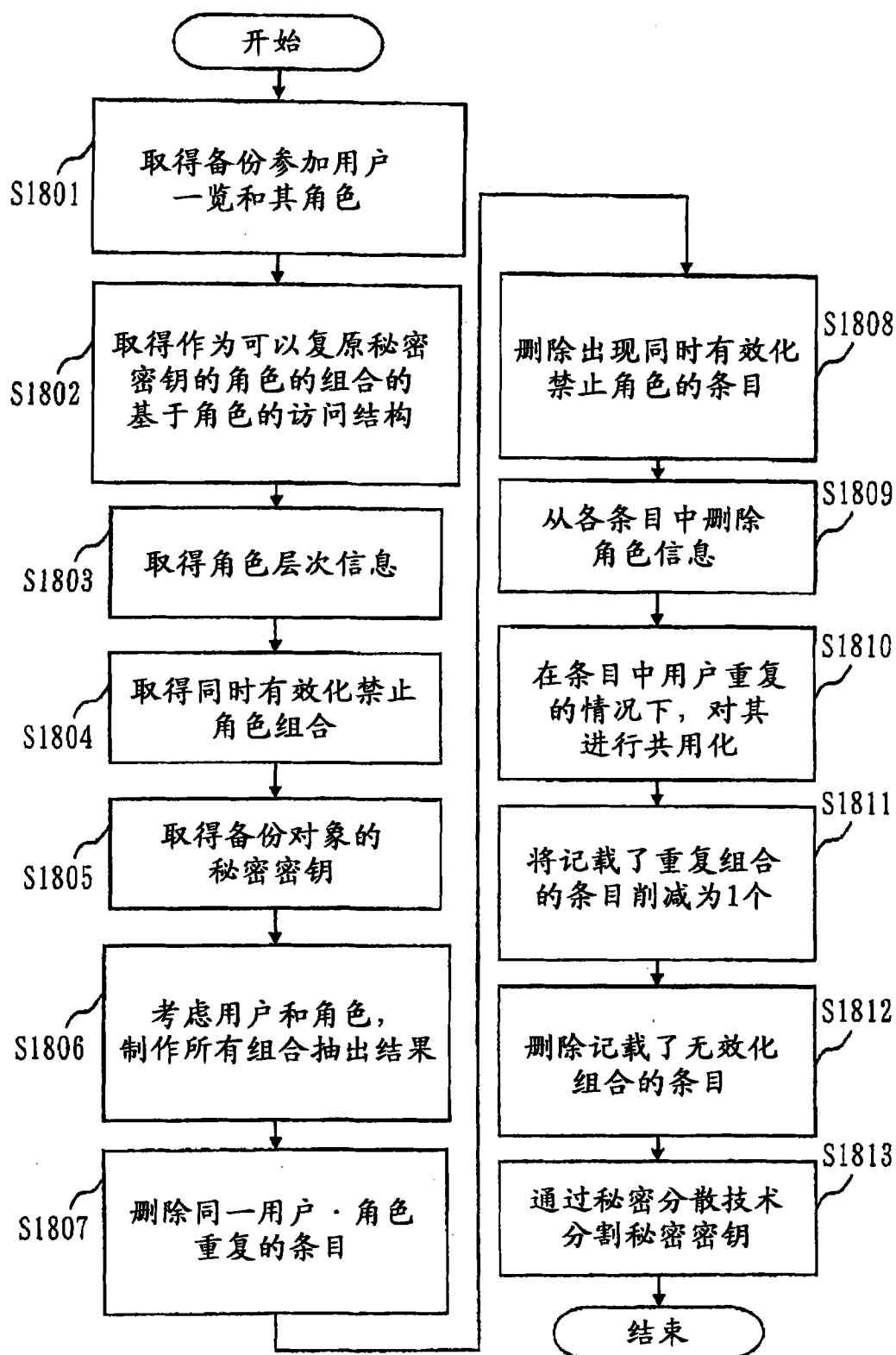


图 18

参加用户名	有效化角色
UserA	RoleD
UserA	RoleB
UserB	RoleB
UserB	RoleC
UserC	RoleC
UserD	RoleA

图 19

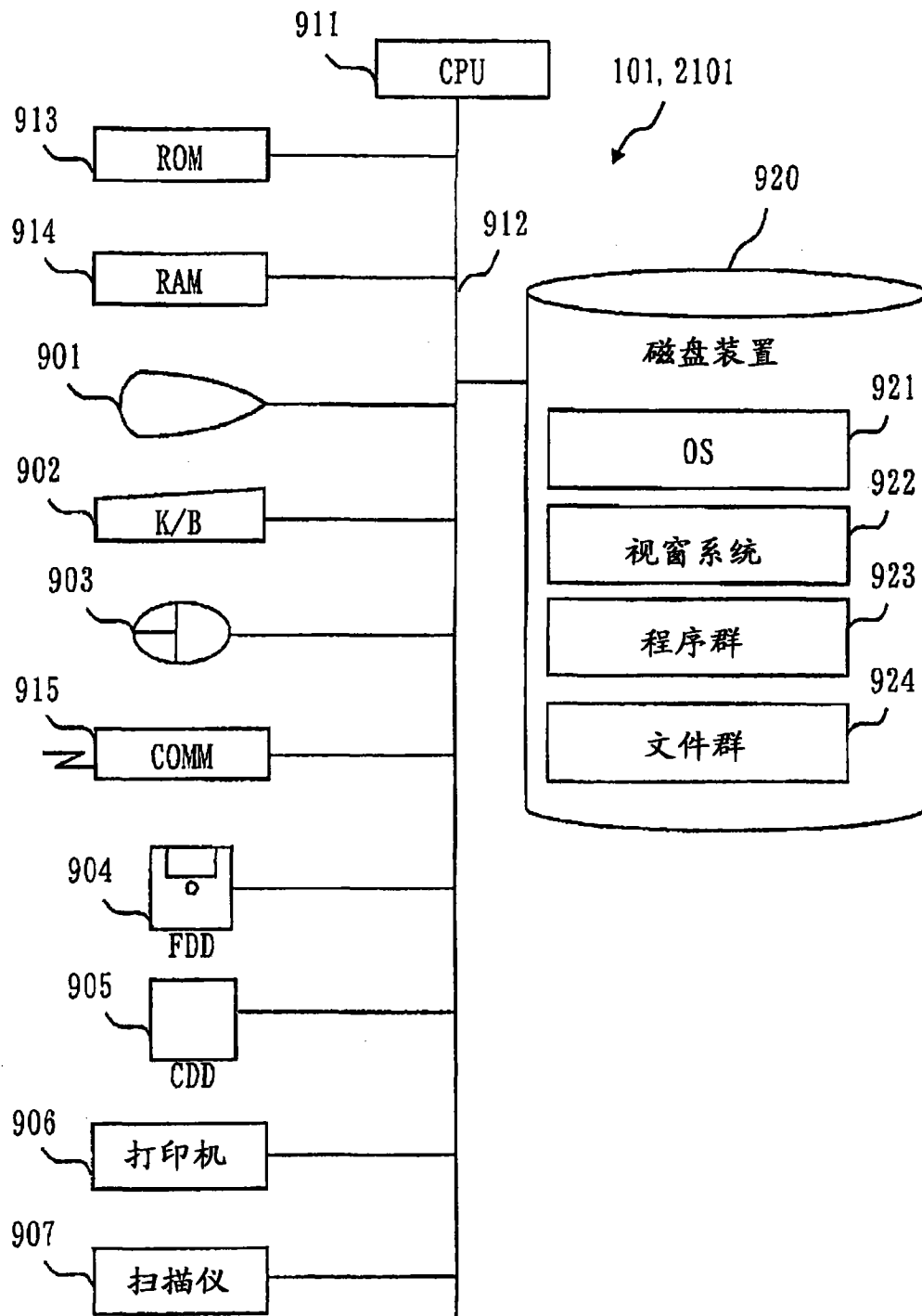


图 20

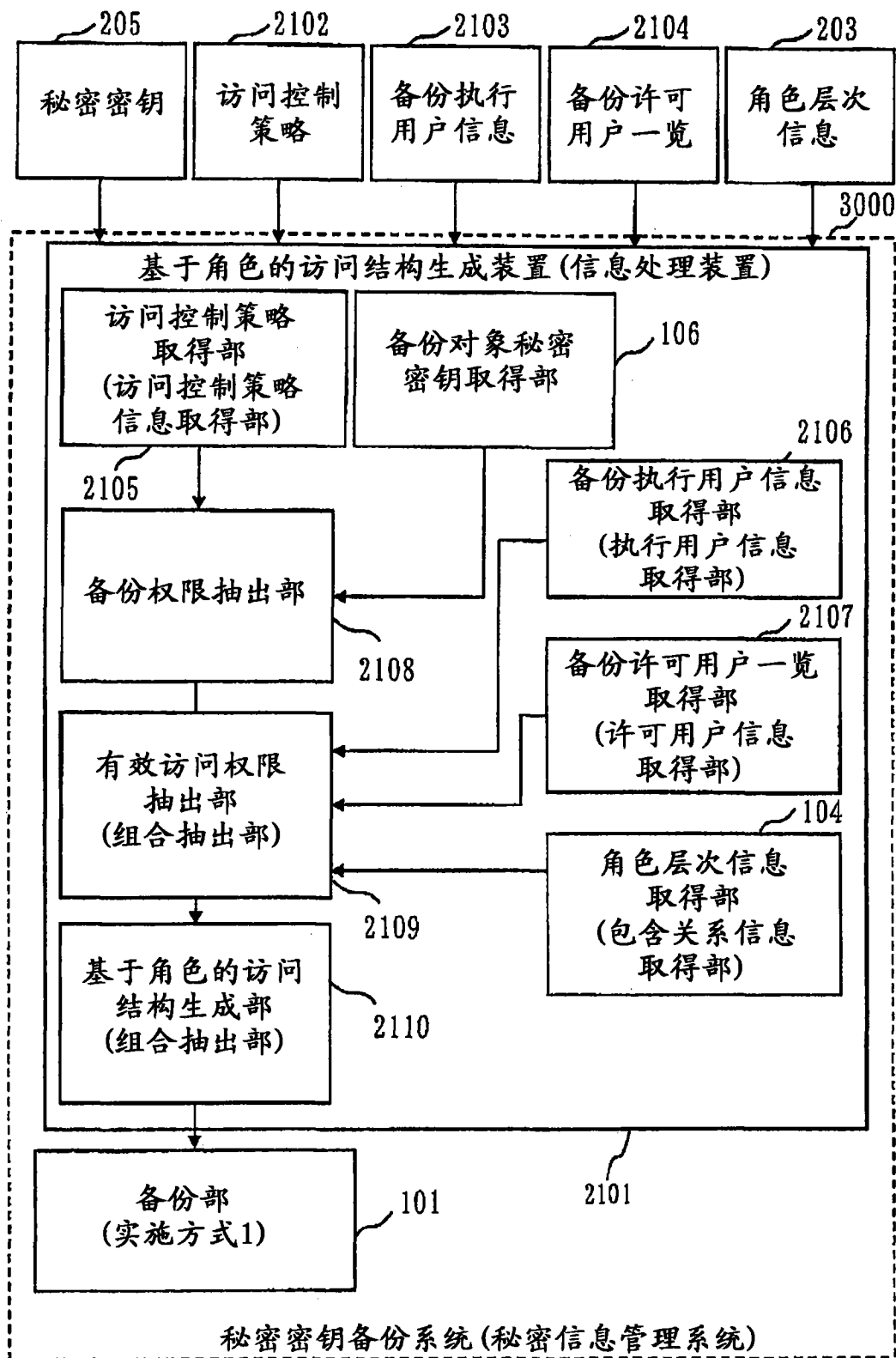


图 21

许可用户名	有效化角色
⋮	⋮

2104

2202

2203

图 22

许可角色名	许可操作 内容	许可操作 对象	许可者 1	⋮	许可者 N
⋮	⋮	⋮	⋮		⋮

2102

2302

2303

2304

2305

图 23

许可角色名	许可操作内容	许可操作对象	许可者1	许可者2
RoleA	备份	秘密密钥1	RoleA	—
RoleA	备份	秘密密钥1	RoleB	RoleC
RoleA	备份	秘密密钥1	RoleB	RoleD
RoleA	备份	秘密密钥1	RoleC	RoleD
RoleA	签名	秘密密钥1	—	—
RoleA	密钥生成	秘密密钥1	RoleB	RoleC
RoleA	密钥生成	秘密密钥1	RoleB	RoleD
RoleA	密钥生成	秘密密钥1	RoleC	RoleD

图 24

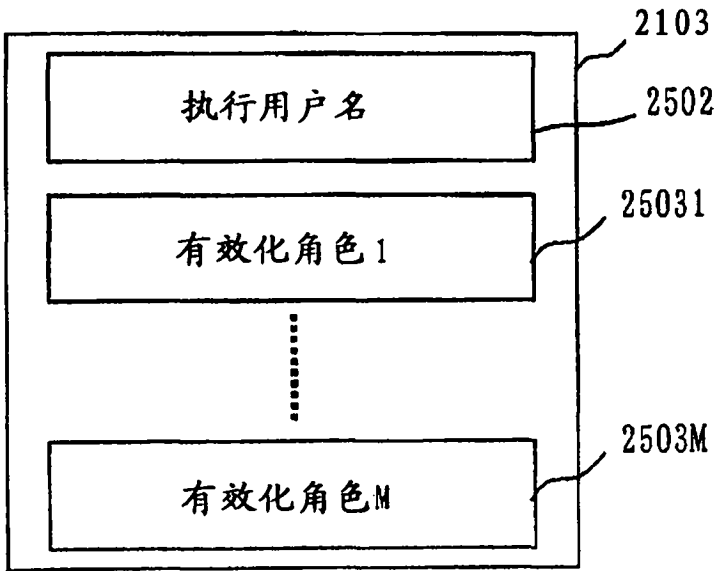


图 25

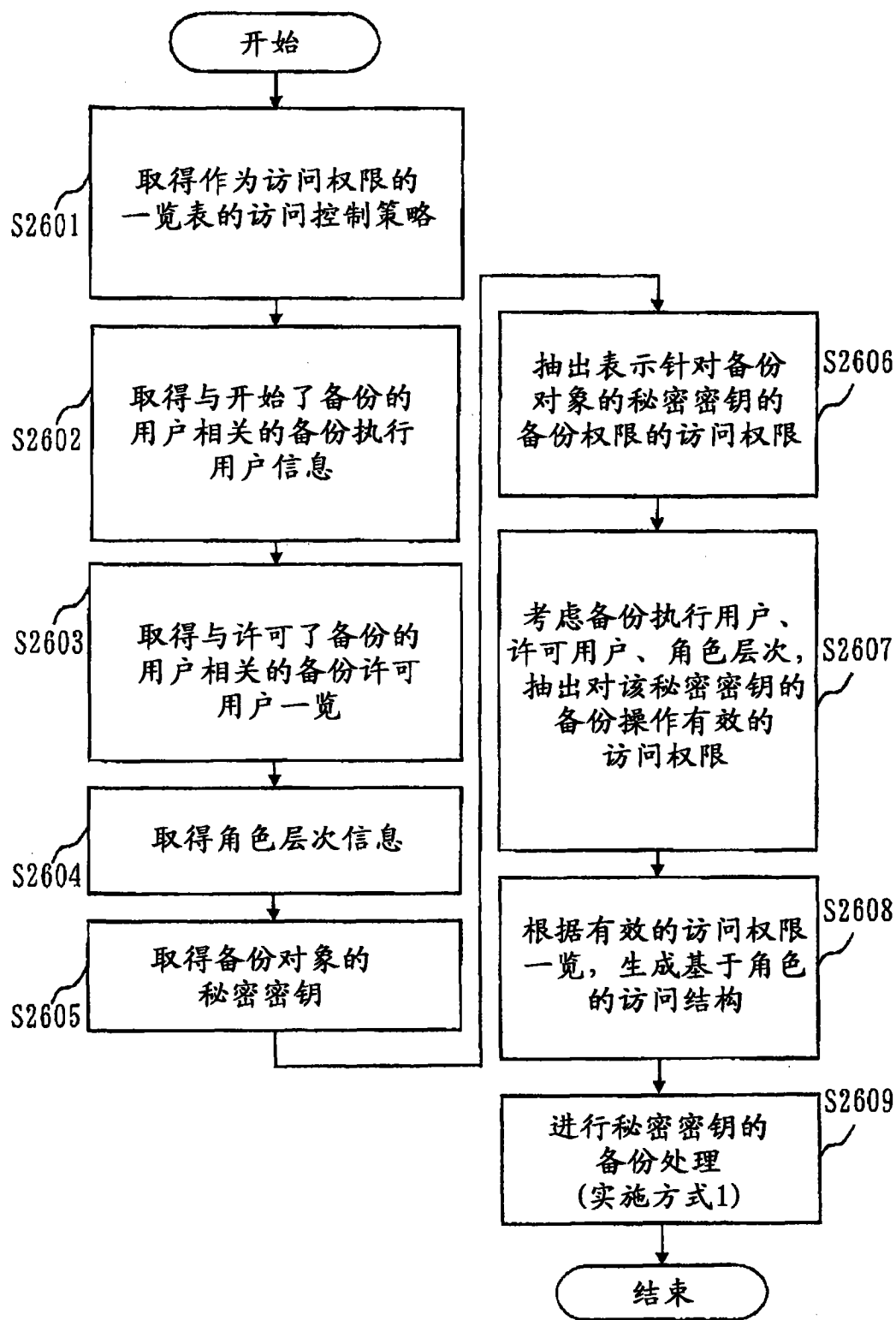


图 26