

明 細 書

発明の名称：秘密分散システム、装置及び記憶媒体

技術分野

[0001] 本発明の実施形態は、秘密分散システム、装置及び記憶媒体に関する。

背景技術

[0002] 近年、電子データに対する情報セキュリティ技術の重要性が高まっている。情報セキュリティ技術は、機密性、完全性及び可用性を担保することを目的としており、最近では、情報漏洩への関心の高まりから、機密性を重視する傾向がみられる。

[0003] 一般に、電子データの機密性を担保する技術としては、暗号化技術が用いられている。暗号化技術は、秘密にしたい電子データ（以下、“秘密情報”と称す）を暗号化することにより、正しい暗号化鍵を知らない場合には、秘密情報の復元を困難にする技術である。

[0004] 図１０は暗号化技術を用いた情報セキュリティシステム３の一例を示す模式図である。

[0005] 始めに、ユーザ端末３００では、制御部３０２が、記憶部３０１内の秘密情報を通信部３０３により保管サーバ装置３２０に送信する。

[0006] 保管サーバ装置３２０は、この秘密情報に対する暗号化保存動作と、暗号化された秘密情報の復号返信動作とを実行する。

[0007] 暗号化保存動作においては、通信部３２３がユーザ端末３００から秘密情報を受信すると、制御部３２２が、この秘密情報を送信したユーザの暗号化鍵を鍵管理部３２４から取得する。暗号化／復号部３２５は、取得された暗号化鍵に基づいて秘密情報を暗号化し、当該暗号化された秘密情報を記憶部３２１に書込む。

[0008] また、復号返信動作においては、通信部３２３がユーザ端末３００から秘密情報読出し要求を受信すると、制御部３２２が、記憶部３２１内の復号鍵を鍵管理部３２４から取得する。この復号鍵は、秘密情報を所有するユーザ

の復号鍵である。暗号化／復号部 325 は、当該取得された復号鍵に基づいて、暗号化された秘密情報を復号し、当該復号された秘密情報を通信部 323 からユーザ端末 300 に返信する。

[0009] このような情報セキュリティシステムにおいて、元の秘密情報を無効化したい場合、鍵管理部内の復号鍵を削除する手法がある。この手法は、保管サーバ装置内にデータのコピーが残っていても、復号鍵が無い場合、秘密情報を復号できない利点がある。しかしながら、暗号化技術は、現在の計算機能力や解読技術での計算量を安全性の根拠とするため、計算機能力や解読技術の進歩により、保管サーバ装置内に残されたデータから秘密情報が復号される心配がある。

[0010] 一方、暗号化技術の他に、電子データの機密性を担保する技術として秘密分散技術が注目されている。秘密分散技術は、秘密情報を分散して複数の分散情報を生成し、これらの分散情報のうち、予め決められた集合を満たす分散情報の集合からは元の秘密情報を復元できるが、予め決められた集合を満たさない分散情報の集合からは元の秘密情報が全く漏洩しないといった特長をもつ技術である。

[0011] 暗号化技術と秘密分散技術とは、暗号化技術の安全性が計算理論的であるのに対し、秘密分散技術の安全性が情報理論的である点で大きく異なる。例えば、暗号化技術は、解読に必要な計算量が多いことを安全性の根拠にするので、計算機能力の向上による情報漏洩の心配がある。これに対し、秘密分散技術は、復元に必要な分散情報が足りないことを安全性の根拠とするので、計算機能力の向上による情報漏洩の心配がない。このように、両者の安全性は大きく異なる。

[0012] 更に、秘密分散技術は、機密性に加え、可用性の担保が可能であり、シャミアにより提案された (k, n) しきい値秘密分散法が代表的である。ここで、 (k, n) しきい値秘密分散法は、秘密情報を n 個の分散情報に分割し、任意の k 個の分散情報からは秘密情報を復元できるが、任意の $(k - 1)$ 個の分散情報からは秘密情報を復元できない手法である。なお、 k と n はそ

それぞれ ($2 \leq k \leq n$) を満たす自然数である。

[0013] このような秘密分散技術は、情報理論的な安全性を確保するため、各分散情報のデータサイズを元の秘密情報のデータサイズよりも小さくできない。

このため、秘密情報を n 個の分散情報に分割した場合、 n 個の分散情報のデータサイズが元の秘密情報の n 倍になるといった不都合が生じる。

[0014] 一方、近年では、第三者のリソース提供者が、例えば、クラウドコンピュータ (Central Processing Unit)、メモリ及びハードディスク (HDD: Hard Disc Drive) 等の計算機資源が適宜、提供される。このようなリソース提供サービスによれば、多量のハードディスクが利用可能となるため、前述したデータサイズの不都合を補うことができる。

[0015] 図 1 はリソース提供サービスを用いた秘密分散システム 4 の一例を示す模式図である。秘密分散システム 4 においては、データラー装置 400 が、ユーザから預かった元の秘密情報を記憶し、この秘密情報の分散処理と配布動作及び復元動作を実行する。保管サーバ装置 420、430、440 は、リソース提供者が所有するサーバ装置である。

[0016] 例えば、分散処理と配布動作の場合、データラー装置 400 では、情報分散部 403 が、制御部 402 の指示に従って、記憶部 401 内の秘密情報に分散処理を実行する。この分散処理は、 $(2, 3)$ しきい値秘密分散法 ($k = 2, n = 3$) に基づくものとする。

[0017] 分散処理の後、データラー装置 400 は、通信部 404 からネットワーク 410 を介して、3 個の分散情報を保管サーバ装置 420、430、440 に各々配布する。

[0018] 保管サーバ装置 420、430、440 は、通信部 422、432、442 を介して自装置宛の分散情報を各々受信し、記憶部 421、431、441 に記憶する。

[0019] また、復元動作の場合、データラー装置 400 は、分散情報読み出し要求を

通信部404からネットワーク410を介して各保管サーバ装置420, 430, 440に送信し、返信された分散情報を受信する。なお、ディーラー装置400は、 k 台($k=2$)以上の保管サーバ装置に分散情報読出し要求を送信する。分散情報読出し要求の送信対象の保管サーバ装置は、ユーザの操作に応じて、任意に選択される。また、情報結合部405は、制御部402の指示に従って、受信された分散情報を結合し、元の秘密情報を復元する。

[0020] このような秘密分散システムにおいて、元の秘密情報を無効化したい場合、 k 台以上の保管サーバ装置内の分散情報を削除する手法がある。

先行技術文献

特許文献

[0021] 特許文献1：特開2009-103774号公報

非特許文献

[0022] 非特許文献1：A. Shamir: "How to share a secret", Communications of the ACM, 22, 11, pp.612-613(1979)

発明の概要

発明が解決しようとする課題

[0023] しかしながら、以上のような秘密分散システムでは、リソース提供者が、可用性の確保やデータ損失の防止といった理由から、保管サーバ装置内の分散情報を所定のタイミングで自動的にコピーし、このコピーされた情報（以下、“複製情報”と称す）を意図しない保管サーバ装置に記憶させることが多い。これにより、ユーザが元の秘密情報を無効化したつもりでも、意図しない保管サーバ装置内に複製情報が残ることから、秘密情報が無効化されないといった不都合が生じる。

[0024] 本発明が解決しようとする課題は、意図しない保管サーバ装置内に複製情報が残っていたとしても、秘密情報を無効化し得る秘密分散システム、装置及び記憶媒体を提供することである。

課題を解決するための手段

- [0025] 実施形態の秘密分散システムは、秘密分散装置、複数の第1保管サーバ装置及び少なくとも1つの第2保管サーバ装置を備えている。
- [0026] 前記秘密分散装置は、秘密情報を分散数 n の個数の分散情報に分散し、当該分散された複数の分散情報のうち、任意のしきい値 k 以上の個数の分散情報から当該秘密情報を復元可能な (k, n) しきい値秘密分散法（但し、 $2 \leq k \leq n$ ）を実行可能である。
- [0027] 前記各第1保管サーバ装置は、前記秘密分散装置から配布された分散情報を個別に記憶する分散情報記憶手段を有し、ユーザの操作に応じて、前記記憶された分散情報の複製処理を制御可能である。
- [0028] 前記第2保管サーバ装置は、前記秘密分散装置から配布された分散情報を個別に記憶する分散情報記憶手段を有し、前記記憶された分散情報の複製処理を所定のタイミングで実行する。
- [0029] 前記秘密分散装置においては、記憶手段が、前記秘密情報を一時的に記憶する。
- [0030] 前記秘密分散装置においては、ユーザの操作に応じて、前記しきい値 k 及び前記分散数 n の入力を受け付ける。
- [0031] 前記秘密分散装置においては、前記受け付けたしきい値 k 及び分散数 n と前記 (k, n) しきい値秘密分散法とに基づいて、前記記憶手段内の秘密情報を n 個の分散情報に分散する。
- [0032] 前記秘密分散装置においては、前記分散された n 個の分散情報のうち、 $n - (k - 1)$ 個以上の分散情報を選択する。
- [0033] 前記秘密分散装置においては、前記選択された分散情報を前記各第1保管サーバ装置に個別に配布する。
- [0034] 前記秘密分散装置においては、前記分散された n 個の分散情報のうち、前記選択された $n - k + 1$ 個の分散情報を除く分散情報を前記第2保管サーバ装置に個別に配布する。
- [0035] 前記秘密分散装置においては、ユーザの操作に応じて、前記各第1保管サ

サーバ装置に配布された分散情報の名称を示す名称情報を含み、当該分散情報と当該分散情報の複製からなる複製情報とを削除するための削除要求を前記各第 1 保管サーバ装置に送信する。

[0036] また、前記各第 1 保管サーバ装置においては、保管位置情報記憶手段が、前記名称情報と、この名称情報により示される分散情報及び複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを関連付けて記憶する。

[0037] 前記各第 1 保管サーバ装置においては、前記秘密分散装置から送信された削除要求を受けると、当該受信した削除要求内の名称情報に基づいて、当該名称情報に関連付けられた保管位置情報を前記保管位置情報記憶手段から読出す。

[0038] 前記各第 1 保管サーバ装置においては、前記読出された保管位置情報に基づいて、前記受信された削除要求内の名称情報により示される分散情報及び複製情報を全て削除する。

図面の簡単な説明

[0039] [図1]図 1 は、第 1 の実施形態における秘密分散システムの構成の一例を示す模式図である。

[図2]図 2 は、同実施形態における保管位置情報記憶部に記憶された情報の一例を示す模式図である。

[図3]図 3 は、同実施形態における保管位置情報記憶部に記憶された情報の一例を示す模式図である。

[図4]図 4 は、同実施形態における秘密分散システムの秘密分散処理の一例を示すフローチャートである。

[図5]図 5 は、同実施形態における秘密分散システムの秘密分散処理の一例を示す模式図である。

[図6]図 6 は、同実施形態における秘密分散システムの秘密情報無効化処理の一例を示すフローチャートである。

[図7]図 7 は、第 2 の実施形態における秘密分散システムの構成の一例を示す

模式図である。

[図8]図8は、同実施形態における保管位置情報記憶部に記憶された情報の一例を示す模式図である。

[図9]図9は、同実施形態における秘密分散システムの秘密情報無効化処理の一例を示すフローチャートである。

[図10]図10は、秘密情報の暗号化／復号化を実現するリソース提供サービスを用いた情報セキュリティシステムの構成の一例を示す模式図である。

[図11]図11は、リソース提供サービスを用いた秘密分散システムの構成の一例を示す模式図である。

発明を実施するための形態

[0040] 以下、各実施形態について図面を参照して説明する。なお、以下の各装置は、装置毎に、ハードウェア構成、又はハードウェア資源とソフトウェアとの組合せ構成のいずれでも実施可能となっている。組合せ構成のソフトウェアとしては、図1、7に示す如き、予めネットワーク又は非一時的なコンピュータ読取可能な記憶媒体 (non-transitory computer-readable storage medium) Mからコンピュータにインストールされ、対応する装置の機能を当該コンピュータに実現させるためのプログラムが用いられる。

[0041] また、本発明は (k, n) しきい値秘密分散法 (但し、 $2 \leq k \leq n$) において、分散情報の確実な削除を行うために、 $n - (k - 1)$ 個の分散情報を第1保管サーバ装置に置いている。そうすることによって、第2保管サーバには分散情報が $k - 1$ 個しかないため復元できない、という特徴がある。従って、第2保管サーバの個数は“ $k - 1$ 個”以下、第1保管サーバの個数は“ $n - (k - 1)$ 個”以上であればよい。ここで、第1保管サーバに多くの分散情報を置くのは、可用性の観点から好ましいとはいえないと考えられるため、以下の各実施の形態では最小の“ $n - (k - 1)$ 個”、即ち“ $n - k + 1$ 個”を例にして記載する。

[0042] (第1の実施形態)

図1は、第1の実施形態における秘密分散システムの構成の一例を示す模

式図である。

[0043] 秘密分散システム 1 では、ディーラー装置 100 が、ネットワーク 110 を介して、2 台の第 1 保管サーバ装置 120, 130 及び 1 台の第 2 保管サーバ装置 140 に接続している。なお、本実施形態では、第 1 保管サーバ装置が 2 台であり、第 2 保管サーバ装置が 1 台である構成としたが、これらの台数に限定されない。

[0044] また、同実施形態において、第 1 保管サーバ装置 120, 130 は、ユーザの操作に応じて、これら保管サーバ装置に記憶された分散情報の複製処理を制御可能である保管サーバ装置を示し、第 2 保管サーバ装置 140 は、この保管サーバ装置に記憶された分散情報の複製処理を所定のタイミングで実行する保管サーバ装置を示している。すなわち、第 1 保管サーバ装置 120, 130 は、ユーザの操作に応じて、ディーラー装置 100 から送信され、保管サーバ装置 120, 130 内の分散情報の名称を示す名称情報を含んで当該分散情報を複製することを要求する複製要求を受けると、当該受信した複製要求に基づいて分散情報の複製処理を実行する。補足すると、第 1 保管サーバ装置 120, 130 は、ディーラー装置 100 から複製要求を受けない場合には、分散情報の複製処理を実行しない。このようなディーラー装置 100 及び第 1 保管サーバ装置 120, 130 は、複製処理を容易に管理し得る観点から、リソース提供者のプライベートクラウドにより実現することが好ましい。なお、「分散情報の名称を示す名称情報」は、秘密情報 s 1 の名称及び分散情報の識別番号 1, 2, 3 を含んで当該分散情報の名称を示す名称情報 s 11, s 12, s 13 としてもよい。また、第 2 保管サーバ装置 140 は、ディーラー装置 100 からの複製要求に基づいて複製処理を実行するのではなく、所定のタイミングで複製処理を自動的に実行する。このような第 2 保管サーバ装置 140 は、複製処理を容易に管理できないパブリッククラウドにより実現することが可能である。

[0045] ディーラー装置 100 は、秘密情報を分散数 n の個数の分散情報に分散し、当該分散された複数の分散情報のうち、任意のしきい値 k 以上の個数の分

散情報から当該秘密情報を復元可能な (k, n) しきい値秘密分散法（但し、 $2 \leq k \leq n$ ）の秘密分散装置を実現するものである。

[0046] なお、ディーラー装置 100 は、 (k, n) しきい値秘密分散法に代えて、例えば、 (n, n) 秘密分散法の秘密分散装置としても実現可能となっている。この場合、 (n, n) 秘密分散法の秘密分散装置を実現するディーラー装置は、ネットワークを介して、1 台の第 1 保管サーバ装置及び $n - 1$ 台の第 2 保管サーバ装置に接続されて用いられる。この詳細については後述する。

[0047] ディーラー装置 100 は、記憶部 101、制御部 102、情報分散部 103、分散情報選択部 104、通信部 105 及び情報結合部 106 を備えている。

[0048] ここで、記憶部 101 は、各部 102 ~ 106 から読出／書込可能な記憶装置であり、秘密情報が一時的に記憶される。また、記憶部 101 は、各部 102 ~ 106 の処理途中のデータや、情報分散部 103 において分散された n 個の分散情報が一時的に記憶されてもよい。

[0049] 制御部 102 は、ユーザの操作に応じて、前述したしきい値 k 及び分散数 n の入力を受け付ける処理を実行する。また、制御部 102 は、各部 103, 104, ..., 106 の動作を制御する処理も実行する。

[0050] 情報分散部 103 は、制御部 102 において受け付けたしきい値 k 及び分散数 n を用いる (k, n) しきい値秘密分散法に基づいて、秘密情報を n 個の分散情報に分散させる処理を実行する。

[0051] 分散情報選択部 104 は、情報分散部 103 において分散された n 個の分散情報のうち、 $n - k + 1$ 個の分散情報を選択する処理を実行する。ここで、 $n - k + 1$ 個の分散情報は、削除された場合に残りの分散情報を $k - 1$ 個（しきい値 k 未満）にする個数を示す $n - (k - 1)$ 個の分散情報を意味している。

[0052] 通信部 105 は、情報分散部 103 において分散された n 個の分散情報を $n - k + 1$ 個の第 1 保管サーバ装置 120, 130 及び $k - 1$ 個の第 2 保管

サーバ装置 140 に配布（例、 $k = 2$ 、 $n = 3$ の場合）し、且つ、各保管サーバ装置 120、130、140 に配布された分散情報を読み出す処理を実行する。また、通信部 105 は、ユーザの操作に応じて、各種要求を各保管サーバ装置 120～140 に個別に送信する処理も実行する。具体的には、以下の各機能(f105-1)～(f105-6)をもっている。

[0053] (f105-1) 分散情報選択部 104 において選択された $n - k + 1$ 個の分散情報を第 1 保管サーバ装置 120、130 に個別に配布する機能。

[0054] (f105-2) 情報分散部 103 において分散された n 個の分散情報のうち、当該選択された $n - k + 1$ 個の分散情報を除く分散情報を第 2 保管サーバ装置 140 に個別に配布する機能。

[0055] (f105-3) ユーザの操作に応じて、第 1 保管サーバ装置 120、130 に配布された分散情報の名称を示す名称情報を含み、当該分散情報と当該分散情報の複製からなる複製情報とを削除するための削除要求を第 1 保管サーバ装置 120、130 に送信する機能。

[0056] (f105-4) ユーザの操作に応じて、第 1 保管サーバ装置 120、130 に配布された分散情報を複製するための複製要求を第 1 保管サーバ装置 120、130 に送信する機能。

[0057] (f105-5) ユーザの操作に応じて、当該配布された各分散情報を読み出すための読み出し要求を各保管サーバ装置 120～140 に送信する機能。

[0058] (f105-6) 各保管サーバ装置 120～140 に送信された読み出し要求に応じて、各保管サーバ装置 120～140 から返信された分散情報を受信する機能。

[0059] 情報結合部 106 は、通信部 105 において受信された分散情報を結合し、元の情報を復元する処理を実行する。換言すると、情報結合部 106 は、通信部 105 において受信された k 個以上の分散情報から (k, n) しきい値秘密分散法に基づいて、秘密情報を復元する処理を実行する。

[0060] 次に、第 1 保管サーバ装置 120、130 及び第 2 保管サーバ装置 140 について説明する。なお、第 1 保管サーバ装置 120、130 は互いに同一

の機能ブロック構成を有するので、以下、第1保管サーバ装置120を代表例に挙げて説明する。

[0061] 第1保管装置120は、分散情報記憶部121、保管位置情報記憶部122、通信部123及び分散情報削除部124を備えている。

[0062] ここで、分散情報記憶部121は、各部123、124から読出／書込可能な記憶装置又は記憶装置の記憶領域であり、ディーラー装置100から配布された分散情報を記憶している。

[0063] 保管位置情報記憶部122は、各部123、124から読出／書込可能な記憶装置又は記憶装置の記憶領域であり、図2に示すように、ディーラー装置100から第1保管サーバ装置120に配布された分散情報の名称を示す名称情報s11、s21、s31と、この名称情報により示される分散情報及び複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを関連付けて記憶している。

[0064] なお、名称情報s11、s21、s31の分散情報は、図2に示すように、第1保管サーバ装置120に記憶されている。名称情報s11の分散情報の複製情報は、図示しないバックアップ装置に記憶されている。また、保管位置情報記憶部122では、第1保管サーバ装置120に分散情報が記憶されると、図3に示すように、名称情報及び保管位置情報“第1保管サーバ装置”を関連付けた新たな行情報が追加される。同様に、保管位置情報記憶部122では、第1保管サーバ装置120に記憶された分散情報が複製されると、名称情報及び保管位置情報“バックアップ装置”を関連付けた新たな行情報が追加される。

[0065] 通信部123は、ディーラー装置100から配布された分散情報を受信すると、当該受信した分散情報を分散情報記憶部121に書込む処理と、当該分散情報の保管位置情報を保管位置情報記憶部122に書込む処理とを実行する。また、通信部123は、ディーラー装置100から送信された各種要求を受信する処理も実行する。具体的には、以下の各機能(f123-1)～(f123-4)をもっている。

- [0066] (f123-1) ディーラー装置 100 から配布された分散情報を受信すると、当該受信した分散情報を分散情報記憶部 121 に書込む機能。
- [0067] (f123-2) ディーラー装置 100 から送信された削除要求を受けると、当該受信した削除要求内の名称情報に基づいて、当該名称情報に関連付けられた保管位置情報を保管位置情報記憶部 122 から読出す機能。
- [0068] (f123-3) ディーラー装置 100 から送信された複製要求を受けると、当該受信した複製要求に基づいて、分散情報記憶部 121 内の分散情報を複製する機能。また、当該複製により得られた複製情報をバックアップ装置（図示せず）に書込む機能と、当該複製情報の保管位置情報を保管位置情報記憶部 122 に書込む機能。
- [0069] (f123-4) ディーラー装置 100 から送信された読出し要求を受けると、当該受信した読出し要求に基づいて、分散情報記憶部 121 から分散情報を読出し、当該読出された分散情報をディーラー装置 100 に返信する機能。
- [0070] 分散情報削除部 124 は、通信部 123 において読出された保管位置情報に基づいて、当該受信された削除要求内の名称情報により示される分散情報及びこの分散情報の複製情報を全て削除する機能をもっている。また、分散情報削除部 124 は、分散情報及びこの分散情報の複製情報を全て削除すると、当該分散情報の名称情報に基づいて、保管位置情報記憶部 122 内の当該名称情報及びこの名称情報に関連付けられた保管位置情報を示す行情報を全て削除する機能をもっている。
- [0071] 第 2 保管サーバ装置 140 は、分散情報記憶部 141 及び通信部 142 を備えている。
- [0072] 分散情報記憶部 141 は、第 1 保管サーバ装置 120 内の分散情報記憶部 121 と同様に、ディーラー装置 100 から配布された分散情報を記憶している。
- [0073] 通信部 142 は、ディーラー装置 100 から個別に配布された分散情報を受信すると、この分散情報を分散情報記憶部 141 に書込む処理を実行する。また、通信部 142 は、ディーラー装置 100 から読出し要求を受信する

と、分散情報記憶部 141 から分散情報を読み出し、この分散情報をディーラー装置 100 に返信する処理を実行する。

[0074] 次に、以上のように構成された秘密分散システムの動作について、図 4 乃至図 6 を参照しながら説明する。始めに、秘密情報の分散処理の動作について、 $k = 2$ 、 $n = 3$ の場合を例に挙げて述べる。

[0075] 制御部 102 は、図 4 に示すように、ユーザの操作に応じて、 (k, n) しきい値秘密分散法のしきい値 k の値 “2” 及び分散数 n の値 “3” の入力を受け付ける（ステップ S1）。

[0076] 続いて、情報分散部 103 は、しきい値 “2” 及び分散数 “3” と $(2, 3)$ しきい値秘密分散法に基づいて、図 5 に示すように、記憶部 101 内の秘密情報 s 1 を 3 個の分散情報に分散し、分散情報 s 11, s 12, s 13 を生成する（ステップ S2）。なお、ステップ S2 において生成された分散情報 s 11, s 12, s 13 は、記憶部 101 に記憶される。

[0077] 次に、分散情報選択部 104 は、生成された 3 個の分散情報のうち、 $n - k + 1$ 個に相当する 2 個の分散情報を選択する（ステップ S3）。ここでは、分散情報選択部 104 は、分散情報 s 11, s 12 を選択したものとする。

[0078] しかる後、通信部 105 は、選択された分散情報 s 11, s 12 を第 1 保管サーバ装置 120, 130 に個別に配布し、残りの分散情報 s 13 を第 2 保管サーバ装置 140 に個別に配布する（ステップ S4）。

[0079] これにより、秘密情報の分散処理が完了する。その後、各保管サーバ装置 120, 130, 140 では、分散情報 s 11, s 12, s 13 の複製処理が適宜、実行される。

[0080] 続いて、秘密情報の無効化処理について説明する。今、ステップ S1～S4 の処理が既に実行され、第 1 保管サーバ装置 120, 130 内には分散情報 s 11, s 12 が記憶され、第 2 保管サーバ装置 140 内には分散情報 s 13 が記憶されているものとする。また、各保管サーバ装置 120, 130, 140 の各バックアップ装置には、分散情報 s 11, s 12, s 13 の複

製情報が記憶されているものとする。

[0081] 始めに、通信部 105 は、ユーザの操作に応じて、第 1 保管サーバ装置 120、130 内の分散情報 s11、s12 を削除するための削除要求を第 1 保管サーバ装置 120、130 に送信する (ステップ S11)。この場合、通信部 105 は、第 1 保管サーバ装置 120 内の分散情報 s11 及び分散情報 s11 の複製情報を削除するために、この分散情報の名称を示す名称情報 “s11” を含む削除要求を第 1 保管サーバ装置 120 に送信する。同様に、通信部 105 は、名称情報 “s12” を含む削除要求を第 1 保管サーバ装置 130 に送信する。

[0082] 第 1 保管サーバ装置 120 内の通信部 123 は、クライアント装置 100 から送信された削除要求を受信する (ステップ S12)。同様に、第 1 保管サーバ装置 130 内の通信部 133 は、クライアント装置 100 から送信された削除要求を受信する。

[0083] 次に、通信部 123 は、当該受信した削除要求内の名称情報 “s11” に基づいて、この名称情報 “s11” に関連付けられた保管位置情報 “第 1 保管サーバ装置” 及び “バックアップ装置” を保管位置情報記憶部 122 から読出す (ステップ S13)。同様に、通信部 133 は、当該受信した削除要求内の名称情報 “s12” に基づいて、この名称情報 “s12” に関連付けられた保管位置情報を保管位置情報記憶部 132 から読出す。

[0084] しかる後、分散情報削除部 124 は、当該読出された保管位置情報 “第 1 保管サーバ装置” 及び “バックアップ装置” に基づいて、分散情報 s11 及び分散情報 s11 の複製情報を全て削除する (ステップ S14)。同様に、分散情報削除部 134 は、当該読出された保管位置情報に基づいて、分散情報 s12 及び分散情報 s12 の複製情報を全て削除する。

[0085] また、分散情報削除部 124 は、分散情報 s11 及び分散情報 s11 の複製情報を全て削除すると、保管位置情報記憶部 122 内の名称情報 “s11” 及びこの名称情報 “s11” に関連付けられた保管位置情報を示す行情報を全て削除する。

[0086] 以上説明した第1の実施形態によれば、複製処理を制御可能な第1保管サーバ装置120、130内に保管位置情報記憶部122、132を設けた構成により、第1保管サーバ装置120、130内の分散情報及び複製情報を管理できるので、削除要求に応じて第1保管サーバ装置120、130内の分散情報及び複製情報を全て削除することができる。

[0087] なお、第1の実施形態は、 (k, n) しきい値秘密分散法に限らず、 $2 \leq k \leq n$ であることから、前述したようにしきい値 k が分散数 n に等しい (n, n) 秘密分散法を用いても実施することができる。この場合、第1保管サーバ装置120は1台あればよく、残りの保管サーバ装置130、140は第2保管サーバ装置130'、140とすればよい。

[0088] また、ステップS1においては、分散数 n の値“3”の入力を受け付ける（しきい値 k の入力は無い）。ステップS2においては、分散数“3”と $(3, 3)$ 秘密分散法に基づいて、前述同様に分散情報 s_{11} 、 s_{12} 、 s_{13} が生成される。ステップS3においては、1個 $(=n-n+1$ 個 $=n-(n-1)$ 個)の分散情報 s_{11} が選択される。ステップS4においては、通信部105は、選択された分散情報 s_{11} を第1保管サーバ装置120に個別に配布し、残りの分散情報 s_{12} 、 s_{13} を第2保管サーバ装置130'、140に個別に配布する。無効化処理においては、第1保管サーバ装置120内には分散情報 s_{11} が記憶され、第2保管サーバ装置130'、140内には分散情報 s_{12} 、 s_{13} が記憶されているものとする。

[0089] そして、各保管サーバ装置120、130'、140の各バックアップ装置には、分散情報 s_{11} 、 s_{12} 、 s_{13} の複製情報が記憶されているものとする。ステップS11～S14において、第1保管サーバ装置120の動作は前述した通りである。但し、 (n, n) 秘密分散法においては、2台目の第1保管サーバ装置130は存在しないので、前述した第1保管サーバ装置130の動作が省略される。

[0090] なお、このように (k, n) しきい値秘密分散法に限らず、 (n, n) 秘密分散法としても実施できることは、以下の各実施形態でも同様である。

[0091] (第2の実施形態)

図7は、第2の実施形態における秘密分散システムの構成の一例を示す模式図であり、図1と同一機能部には同一符号を付してその詳しい説明を省略し、ここでは異なる機能部について主に述べる。なお、以下の各実施形態も同様にして重複した説明を省略する。

[0092] 第2の実施形態は、第1の実施形態の変形例であり、図1に示した構成とは異なり、第1保管サーバ装置120、130内の保管位置情報記憶部122、132に代えて、保管位置情報記憶部107をディーラー装置100に設けた構成を示している。

[0093] すなわち、ディーラー装置100は、記憶部101、制御部102、情報分散部103、分散情報選択部104、通信部105a、情報結合部106及び保管位置情報記憶部107を備えている。

[0094] ここで、記憶部101に記憶される情報や、制御部102、情報分散部103、分散情報選択部104及び情報結合部106の機能は、前述した通りである。

[0095] 保管位置情報記憶部107は、図8に示すように、第1保管サーバ装置120、130に配布される分散情報の名称を示す名称情報と、この名称情報により示される分散情報及びこの分散情報の複製からなる複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを関連付けて記憶している。すなわち、保管位置情報記憶部107は、図8に示すように、1台の第1保管サーバ装置120又は130だけでなく、全ての第1保管サーバ装置120、130に記憶された分散情報及び複製情報の名称情報及び保管位置情報を記憶している。

[0096] また、通信部105aは、前述した通信部105の機能(f105-3)の代わりに、例えば、以下の機能(f105a-1)をもっている。なお、通信部105aは、前述した通信部105の各機能(f105-1)、(f105-2)、(f105-4)～(f105-6)と同一の機能ももっている。

[0097] 更に、通信部105aは、削除要求及び複製要求を第1保管サーバ装置1

20, 130に送信すると、保管位置情報記憶部107に記憶された名称情報及び保管位置情報の行情報を更新する処理も実行する。具体的には、例えば、以下の各機能(f105a-2)及び(f105a-3)をもっている。

[0098] (f105a-1) ユーザの操作に応じて、保管位置情報記憶部107に記憶された名称情報及び当該名称情報に関連付けられた保管位置情報を読み出し、当該読み出された名称情報及び保管位置情報を含み、当該配布された分散情報と当該分散情報の複製情報とを削除するための削除要求を第1保管サーバ装置120, 130に送信する機能。

[0099] (f105a-2) ユーザの操作に応じて、名称情報及び保管位置情報を含み、第1保管サーバ装置120, 130内の分散情報と複製情報とを削除するための削除要求を送信すると、この削除要求内の名称情報及び保管位置情報の行情報を保管位置情報記憶部107から削除する機能。

[0100] (f105a-3) ユーザの操作に応じて、第1保管サーバ装置120, 130内の分散情報を複製するための複製要求を送信すると、当該送信された複製要求に基づいて、名称情報及び保管位置情報の行情報を保管位置情報記憶部107に関連付けて書込む機能。

[0101] 次に、第1保管サーバ装置120, 130及び第2保管サーバ装置140について説明する。なお、第1保管サーバ装置120, 130は互いに同一の機能ブロック構成を有するので、以下、第1保管サーバ装置120を代表例に挙げて説明する。また、第2保管サーバ装置140の構成は前述した通りである。

[0102] 第1保管サーバ装置120は、分散情報記憶部121、通信部123a及び分散情報削除部124を備えている。

[0103] ここで、分散情報記憶部121に記憶される情報は、前述した通りである。

[0104] 通信部123aは、前述した通信部123の機能(f123-2)の代わりに、ディーラー装置100から送信された削除要求を受信する処理を実行する機能を有する。

- [0105] 分散情報削除部 123 は、通信部 123a において受信された削除要求内の保管位置情報に基づいて、当該削除要求内の名称情報により示される分散情報及び複製情報を全て削除する機能をもっている。
- [0106] 次に、以上のように構成された秘密分散システムの動作について、前述した図 4 及び新たな図 9 のフローチャートを参照しながら説明する。
- [0107] 始めに、秘密情報の分散処理の動作については、図 4 に示したステップ S1 ～ S4 の動作が前述同様に実行される。但し、ステップ S4 の直前又は直後に、通信部 105a は、第 1 保管サーバ装置 120、130 に配布される分散情報の名称を示す名称情報と、この名称情報により示される分散情報が記憶される場所を個別に示す保管位置情報とを関連付けて保管位置情報記憶部 107 に書き込む。
- [0108] これにより、秘密情報の分散処理が完了する。
- [0109] 続いて、秘密情報の無効化処理について説明する。今、ステップ S1 ～ S4 の処理が既に実行され、第 1 保管サーバ装置 120、130 内には分散情報 s11、s12 が記憶され、第 2 保管サーバ装置 140 内には分散情報 s13 が記憶されているものとする。また同様に、各保管サーバ装置 120、130、140 の各バックアップ装置には、分散情報 s11、s12、s13 の複製情報が記憶されているものとする。
- [0110] 始めに、通信部 105a は、図 9 に示すように、ユーザの操作に応じて、保管位置情報記憶部 107 に記憶された名称情報及び当該名称情報に関連付けられた保管位置情報を読み出し（ステップ S21）、当該読み出された名称情報及び保管位置情報を含み、当該配布された分散情報と当該分散情報の複製情報とを削除するための削除要求を第 1 保管サーバ装置 120、130 に送信する（ステップ S22）。この場合、通信部 105a は、第 1 保管サーバ装置 120 内の分散情報 s11 及び分散情報 s11 の複製情報を削除するために、この分散情報の名称を示す名称情報 “s11” 及び保管位置情報を含む削除要求を第 1 保管サーバ装置 120 に送信する。同様に、通信部 105a は、名称情報 “s12” 及び保管位置情報を含む削除要求を第 1 保管サー

バ装置 130 に送信する。また、通信部 105a は、削除要求を送信すると、この削除要求内の名称情報及びこの名称情報に関連付けられた保管位置情報を示す行情報を全て削除する。

[0111] 一方、第 1 保管サーバ装置 120 内の通信部 123a は、ディーラー装置 100 から送信された削除要求を受信する（ステップ S23）。同様に、第 1 保管サーバ装置 130 内の通信部 133a は、ディーラー装置 100 から送信された削除要求を受信する。

[0112] 次に、分散情報削除部 124 は、通信部 123a に受信された削除要求内の保管位置情報“第 1 保管サーバ装置”及び“バックアップ装置”に基づいて、分散情報 s11 及び分散情報 s11 の複製情報を全て削除する（ステップ S24）。同様に、分散情報削除部 134 は、通信部 133a に受信された保管位置情報に基づいて、分散情報 s12 及び分散情報 s12 の複製情報を全て削除する。

[0113] 以上説明した第 2 の実施形態によれば、ディーラー装置 100 内に保管位置情報記憶部 107 を設けた構成により、第 1 保管サーバ装置 120、130 に記憶された分散情報と複製情報との個数及びこれら分散情報と複製情報との保管場所をディーラー装置 100 内で管理することができる。

[0114] また、第 2 実施形態は、前述同様に、 (k, n) しきい値秘密分散法に限らず、 (n, n) 秘密分散法を用いても実施することができる。この場合、ステップ S1～S4 においては、前述した (n, n) 秘密分散法の例と同様に実施できる。無効化処理においても前述同様に、第 1 保管サーバ装置 120 内には分散情報 s11 が記憶され、第 2 保管サーバ装置 130'、140 内には分散情報 s12、s13 が記憶されているものとする。また同様に、各保管サーバ装置 120、130'、140 の各バックアップ装置には、分散情報 s11、s12、s13 の複製情報が記憶されているものとする。ステップ S21～S24 において、第 1 保管サーバ装置 120 の動作は第 2 の実施形態に述べた通りである。但し、 (n, n) 秘密分散法においては、2 台目の第 1 保管サーバ装置 130 は存在しないので、前述した第 1 保管サー

バ装置 130（内の各部 133a, 134）の動作が省略される。なお、このように（k, n）しきい値秘密分散法に限らず、（n, n）秘密分散法としても実施できることは、前述した通りである。

[0115] 以上説明した少なくともひとつの実施形態によれば、複製処理を制御可能な第1保管サーバ装置と複製処理を自動的に実行する第2保管サーバ装置とを併用したシステム構成により、第2保管サーバ装置内に複製情報が残っていたとしても、元の秘密情報を無効化することができる。

[0116] なお、上記の各実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（CD-ROM、DVDなど）、光磁気ディスク（MO）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

[0117] また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

[0118] また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が上記実施形態を実現するための各処理の一部を実行しても良い。

[0119] さらに、各実施形態における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

[0120] また、記憶媒体は1つに限らず、複数の媒体から上記の各実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

[0121] なお、各実施形態におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、上記の各実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシス

テム等の何れの構成であっても良い。

[0122] また、各実施形態におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

[0123] なお、本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

[請求項1]

秘密情報を分散数 n の個数の分散情報に分散し、当該分散された複数の分散情報のうち、任意のしきい値 k 以上の個数の分散情報から当該秘密情報を復元可能な (k, n) しきい値秘密分散法（但し、 $2 \leq k \leq n$ ）を実行可能な秘密分散装置と、

前記秘密分散装置から配布された分散情報を個別に記憶する分散情報記憶手段を有し、ユーザの操作に応じて、前記記憶された分散情報の複製処理を制御可能な複数の第1保管サーバ装置と、

前記秘密分散装置から配布された分散情報を個別に記憶する分散情報記憶手段を有し、当該記憶された分散情報の複製処理を所定のタイミングで実行する少なくとも1つの第2保管サーバ装置と

を備えた秘密分散システムであって、

前記秘密分散装置は、

前記秘密情報を一時的に記憶する記憶手段と、

ユーザの操作に応じて、前記しきい値 k 及び前記分散数 n の入力を受け付ける手段と、

前記受け付けたしきい値 k 及び分散数 n と前記 (k, n) しきい値秘密分散法とに基づいて、前記記憶手段内の秘密情報を n 個の分散情報に分散する手段と、

前記分散された n 個の分散情報のうち、 $n - (k - 1)$ 個以上の分散情報を選択する手段と、

前記選択された分散情報を前記各第1保管サーバ装置に個別に配布する手段と、

前記分散された n 個の分散情報のうち、前記選択された $n - (k - 1)$ 個以上の分散情報を除く分散情報を前記第2保管サーバ装置に個別に配布する手段と、

ユーザの操作に応じて、前記各第1保管サーバ装置に配布された分散情報の名称を示す名称情報を含み、当該分散情報と当該分散情報の

複製からなる複製情報とを削除するための削除要求を前記各第 1 保管サーバ装置に送信する手段と

を備え、

前記各第 1 保管サーバ装置は、

前記名称情報と、この名称情報により示される分散情報及び複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを関連付けて記憶する保管位置情報記憶手段と、

前記秘密分散装置から送信された削除要求を受けると、当該受信した削除要求内の名称情報に基づいて、当該名称情報に関連付けられた保管位置情報を前記保管位置情報記憶手段から読出す手段と、

前記読出された保管位置情報に基づいて、前記受信された削除要求内の名称情報により示される分散情報及び複製情報を全て削除する手段と

を備えたことを特徴とする秘密分散システム。

[請求項2]

秘密情報を分散数 n の個数の分散情報に分散し、当該分散された複数の分散情報のうち、任意のしきい値 k 以上の個数の分散情報から当該秘密情報を復元可能な (k, n) しきい値秘密分散法（但し、 $2 \leq k \leq n$ ）を実行可能な秘密分散装置と、

前記秘密分散装置から配布された分散情報を個別に記憶する分散情報記憶手段を有し、ユーザの操作に応じて、前記記憶された分散情報の複製処理を制御可能な複数の第 1 保管サーバ装置と、

前記秘密分散装置から配布された分散情報を個別に記憶する分散情報記憶手段を有し、当該記憶された分散情報の複製処理を所定のタイミングで実行する少なくとも 1 つの第 2 保管サーバ装置と

を備えた秘密分散システムであって、

前記秘密分散装置は、

前記秘密情報を一時的に記憶する記憶手段と、

前記各第 1 保管サーバ装置に配布される分散情報の名称を示す名称

情報と、この名称情報により示される分散情報及びこの分散情報の複製からなる複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを関連付けて記憶する保管位置情報記憶手段と、

ユーザの操作に応じて、前記しきい値 k 及び前記分散数 n の入力を受け付ける手段と、

前記受け付けたしきい値 k 及び分散数 n と前記 (k, n) しきい値秘密分散法とに基づいて、前記記憶手段内の秘密情報を n 個の分散情報に分散する手段と、

前記分散された n 個の分散情報のうち、 $n - (k - 1)$ 個以上の分散情報を選択する手段と、

前記選択された分散情報を前記各第 1 保管サーバ装置に個別に配布する手段と、

前記分散された n 個の分散情報のうち、前記選択された $n - (k - 1)$ 個以上の分散情報を除く分散情報を前記第 2 保管サーバ装置に個別に配布する手段と、

ユーザの操作に応じて、前記記憶された名称情報及び当該名称情報に関連付けられた保管位置情報を読み出し、当該読み出された名称情報及び保管位置情報を含み、前記配布された分散情報と当該分散情報の複製情報とを削除するための削除要求を前記各第 1 保管サーバ装置に送信する手段と

を備え、

前記各第 1 保管サーバ装置は、

前記秘密分散装置から送信された削除要求を受けると、当該受信した削除要求内の保管位置情報に基づいて、当該削除要求内の名称情報により示される分散情報及び複製情報を全て削除する手段と

を備えたことを特徴とする秘密分散システム。

[請求項3]

配布された分散情報を個別に記憶する分散情報記憶手段を有し、ユーザの操作に応じて、前記記憶された分散情報の複製処理を制御可能

な複数の第1保管サーバ装置と、配布された分散情報を個別に記憶する分散情報記憶手段を有し、前記記憶された分散情報の複製処理を所定のタイミングで実行する少なくとも1つの第2保管サーバ装置とにそれぞれ通信可能であり、秘密情報を分散数 n の個数の分散情報に分散し、当該分散された複数の分散情報のうち、任意のしきい値 k 以上の個数の分散情報から当該秘密情報を復元可能な (k, n) しきい値秘密分散法（但し、 $2 \leq k \leq n$ ）を実行可能な秘密分散装置であって、

前記秘密情報を一時的に記憶する記憶手段と、

前記各第1保管サーバ装置に配布される分散情報の名称を示す名称情報と、この名称情報により示される分散情報及びこの分散情報の複製からなる複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを関連付けて記憶する保管位置情報記憶手段と、

ユーザの操作に応じて、前記しきい値 k 及び前記分散数 n の入力を受け付ける手段と、

前記受け付けたしきい値 k 及び分散数 n と前記 (k, n) しきい値秘密分散法とに基づいて、前記記憶手段内の秘密情報を n 個の分散情報に分散する手段と、

前記分散された n 個の分散情報のうち、 $n - (k - 1)$ 個以上の分散情報を選択する手段と、

前記選択された分散情報を前記各第1保管サーバ装置に個別に配布する手段と、

前記分散された n 個の分散情報のうち、前記選択された $n - (k - 1)$ 個以上の分散情報を除く分散情報を前記第2保管サーバ装置に個別に配布する手段と、

ユーザの操作に応じて、前記記憶された名称情報及び当該名称情報に関連付けられた保管位置情報を読み出し、当該読み出された名称情報及び保管位置情報を含み、前記配布された分散情報と当該分散情報の複

製情報とを削除するための削除要求を前記各第 1 保管サーバ装置に送信する手段と

を備えたことを特徴とする秘密分散装置。

[請求項4]

配布された分散情報を個別に記憶する分散情報記憶手段を有し、ユーザの操作に応じて、前記記憶された分散情報の複製処理を制御可能な複数の第 1 保管サーバ装置と、配布された分散情報を個別に記憶する分散情報記憶手段を有し、前記記憶された分散情報の複製処理を所定のタイミングで実行する少なくとも 1 つの第 2 保管サーバ装置とにそれぞれ通信可能であり、秘密情報を分散数 n の個数の分散情報に分散し、当該分散された複数の分散情報のうち、任意のしきい値 d 以上の個数の分散情報から当該秘密情報を復元可能な (k, n) しきい値秘密分散法（但し、 $2 \leq k \leq n$ ）を実行可能であり、記憶手段及び保管位置情報記憶手段を備えた秘密分散装置のプロセッサにより実行されるプログラムを記憶した非一時的なコンピュータ読取可能な記憶媒体であって、

前記プログラムは、

前記秘密情報を一時的に前記記憶手段に書込む処理を前記プロセッサに実行させる第 1 プログラムコードと、

前記各第 1 保管サーバ装置に配布される分散情報の名称を示す名称情報と、この名称情報により示される分散情報及びこの分散情報の複製からなる複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを前記保管位置情報記憶手段に関連付けて書込む処理を前記プロセッサに実行させる第 2 プログラムコードと、

ユーザの操作に応じて、前記しきい値 k 及び前記分散数 n の入力を受け付ける処理を前記プロセッサに実行させる第 3 プログラムコードと、

前記受け付けたしきい値 k 及び分散数 n と前記 (k, n) しきい値秘密分散法とに基づいて、前記記憶手段内の秘密情報を n 個の分散情

報に分散する処理を前記プロセッサに実行させる第4プログラムコードと、

前記分散された n 個の分散情報のうち、 $n - (k - 1)$ 個以上の分散情報を選択する処理を前記プロセッサに実行させる第5プログラムコードと、

前記選択された分散情報を前記各第1保管サーバ装置に個別に配布する処理を前記プロセッサに実行させる第6プログラムコードと、

前記分散された n 個の分散情報のうち、前記選択された $n - (k - 1)$ 個以上の分散情報を除く分散情報を前記第2保管サーバ装置に個別に配布する処理を前記プロセッサに実行させる第7プログラムコードと、

ユーザの操作に応じて、前記記憶された名称情報及び当該名称情報に関連付けられた保管位置情報を読み出し、当該読み出された名称情報及び保管位置情報を含み、前記配布された分散情報と当該分散情報の複製情報とを削除するための削除要求を前記各第1保管サーバ装置に送信する処理を前記プロセッサに実行させる第8プログラムコードと

を備えたことを特徴とする記憶媒体。

[請求項5]

秘密情報を分散数 n の個数の分散情報に分散し、当該分散された全ての分散情報から当該秘密情報を復元可能な (n, n) 秘密分散法（但し、 $3 \leq n$ ）を実行可能な秘密分散装置と、

前記秘密分散装置から配布された分散情報を個別に記憶する分散情報記憶手段を有し、ユーザの操作に応じて、前記記憶された分散情報の複製処理を制御可能な第1保管サーバ装置と、

前記秘密分散装置から配布された分散情報を個別に記憶する分散情報記憶手段を有し、当該記憶された分散情報の複製処理を所定のタイミングで実行する複数の第2保管サーバ装置と

を備えた秘密分散システムであって、

前記秘密分散装置は、

前記秘密情報を一時的に記憶する記憶手段と、
ユーザの操作に応じて、前記分散数 n の入力を受け付ける手段と、
前記受け付けた分散数 n 及び前記 (n, n) 秘密分散法に基づいて、
前記記憶手段内の秘密情報を n 個の分散情報に分散する手段と、
前記分散された n 個の分散情報のうち、1 個の分散情報を選択する手段と、
前記選択された分散情報を前記第 1 保管サーバ装置に配布する手段と、
前記分散された n 個の分散情報のうち、前記選択された分散情報を除く分散情報を前記各第 2 保管サーバ装置に個別に配布する手段と、
ユーザの操作に応じて、前記第 1 保管サーバ装置に配布された分散情報の名称を示す名称情報を含み、当該分散情報と当該分散情報の複製からなる複製情報とを削除するための削除要求を前記第 1 保管サーバ装置に送信する手段と
を備え、
前記第 1 保管サーバ装置は、
前記名称情報と、この名称情報により示される分散情報及び複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを関連付けて記憶する保管位置情報記憶手段と、
前記秘密分散装置から送信された削除要求を受けると、当該受信した削除要求内の名称情報に基づいて、当該名称情報に関連付けられた保管位置情報を前記保管位置情報記憶手段から読出す手段と、
前記読出された保管位置情報に基づいて、前記受信された削除要求内の名称情報により示される分散情報及び複製情報を全て削除する手段と
を備えたことを特徴とする秘密分散システム。

[請求項6]

秘密情報を分散数 n の個数の分散情報に分散し、当該分散された全ての分散情報から当該秘密情報を復元可能な (n, n) 秘密分散法（

但し、 $3 \leq n$) を実現可能な秘密分散装置と、

前記秘密分散装置から配布された分散情報を個別に記憶する分散情報記憶手段を有し、ユーザの操作に応じて、前記記憶された分散情報の複製処理を制御可能な第1保管サーバ装置と、

前記秘密分散装置から配布された分散情報を個別に記憶する分散情報記憶手段を有し、前記記憶された分散情報の複製処理を所定のタイミングで実行する複数の第2保管サーバ装置と

を備えた秘密分散システムであって、

前記秘密分散装置は、

前記秘密情報を一時的に記憶する記憶手段と、

前記第1保管サーバ装置に配布される分散情報の名称を示す名称情報と、この名称情報により示される分散情報及びこの分散情報の複製からなる複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを関連付けて記憶する保管位置情報記憶手段と、

ユーザの操作に応じて、前記分散数 n の入力を受け付ける手段と、

前記受け付けた分散数 n 及び前記 (n, n) 秘密分散法に基づいて、前記記憶手段内の秘密情報を n 個の分散情報に分散する手段と、

前記分散された n 個の分散情報のうち、1個の分散情報を選択する手段と、

前記選択された分散情報を前記第1保管サーバ装置に配布する手段と、

前記分散された n 個の分散情報のうち、前記選択された分散情報を除く分散情報を前記各第2保管サーバ装置に個別に配布する手段と、

ユーザの操作に応じて、前記記憶された名称情報及び当該名称情報に関連付けられた保管位置情報を読み出し、当該読み出された名称情報及び保管位置情報を含み、前記配布された分散情報と当該分散情報の複製情報とを削除するための削除要求を前記第1保管サーバ装置に送信する手段と

を備え、

前記第 1 保管サーバ装置は、

前記秘密分散装置から送信された削除要求を受けると、当該受信した削除要求内の保管位置情報に基づいて、当該削除要求内の名称情報により示される分散情報及び複製情報を全て削除する手段と
を備えたことを特徴とする秘密分散システム。

[請求項7]

配布された分散情報を個別に記憶する分散情報記憶手段を有し、ユーザの操作に応じて、前記記憶された分散情報の複製処理を制御可能な第 1 保管サーバ装置と、配布された分散情報を個別に記憶する分散情報記憶手段を有し、前記記憶された分散情報の複製処理を所定のタイミングで実行する複数の第 2 保管サーバ装置とにそれぞれ通信可能であり、秘密情報を分散数 n の個数の分散情報に分散し、当該分散された全ての分散情報から当該秘密情報を復元可能な (n, n) 秘密分散法（但し、 $3 \leq n$ ）を実行可能な秘密分散装置であって、

前記秘密情報を一時的に記憶する記憶手段と、

前記第 1 保管サーバ装置に配布される分散情報の名称を示す名称情報と、この名称情報により示される分散情報及びこの分散情報の複製からなる複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを関連付けて記憶する保管位置情報記憶手段と、

ユーザの操作に応じて、前記分散数 n の入力を受け付ける手段と、

前記受け付けた分散数 n 及び前記 (n, n) 秘密分散法に基づいて、前記記憶手段内の秘密情報を n 個の分散情報に分散する手段と、

前記分散された n 個の分散情報のうち、1 個の分散情報を選択する手段と、

前記選択された分散情報を前記第 1 保管サーバ装置に配布する手段と、

前記分散された n 個の分散情報のうち、前記選択された分散情報を除く分散情報を前記各第 2 保管サーバ装置に個別に配布する手段と、

ユーザの操作に応じて、前記記憶された名称情報及び当該名称情報に関連付けられた保管位置情報を読み出し、当該読み出された名称情報及び保管位置情報を含み、前記配布された分散情報と当該分散情報の複製情報とを削除するための削除要求を前記第 1 保管サーバ装置に送信する手段と

を備えたことを特徴とする秘密分散装置。

[請求項8]

配布された分散情報を個別に記憶する分散情報記憶手段を有し、ユーザの操作に応じて、前記記憶された分散情報の複製処理を制御可能な第 1 保管サーバ装置と、配布された分散情報を個別に記憶する分散情報記憶手段を有し、前記記憶された分散情報の複製処理を所定のタイミングで実行する複数の第 2 保管サーバ装置とにそれぞれ通信可能であり、秘密情報を分散数 n の個数の分散情報に分散し、当該分散された全ての分散情報から当該秘密情報を復元可能な (n, n) 秘密分散法（但し、 $3 \leq n$ ）を実行可能であり、記憶手段及び保管位置情報記憶手段を備えた秘密分散装置のプロセッサにより実行されるプログラムを記憶した非一時的なコンピュータ読み取り可能な記憶媒体であって、

前記プログラムは、

前記秘密情報を一時的に前記記憶手段に書き込む処理を前記プロセッサに実行させる第 9 プログラムコードと、

前記第 1 保管サーバ装置に配布される分散情報の名称を示す名称情報と、この名称情報により示される分散情報及びこの分散情報の複製からなる複製情報がそれぞれ記憶されている場所を個別に示す保管位置情報とを前記保管位置情報記憶手段に関連付けて書き込む処理を前記プロセッサに実行させる第 10 プログラムコードと、

ユーザの操作に応じて、前記分散数 n の入力を受け付ける処理を前記プロセッサに実行させる第 11 プログラムコードと、

前記受け付けた分散数 n 及び前記 (n, n) 秘密分散法に基づいて

、前記記憶手段内の秘密情報を n 個の分散情報に分散する処理を前記プロセッサに実行させる第 1 2 プログラムコードと、

前記分散された n 個の分散情報のうち、1 個の分散情報を選択する処理を前記プロセッサに実行させる第 1 3 プログラムコードと、

前記選択された分散情報を前記第 1 保管サーバ装置に配布する処理を前記プロセッサに実行させる第 1 4 プログラムコードと、

前記分散された n 個の分散情報のうち、前記選択された分散情報を除く分散情報を前記各第 2 保管サーバ装置に個別に配布する処理を前記プロセッサに実行させる第 1 5 プログラムコードと、

ユーザの操作に応じて、前記記憶された名称情報及び当該名称情報に関連付けられた保管位置情報を読み出し、当該読み出された名称情報及び保管位置情報を含み、前記配布された分散情報と当該分散情報の複製情報とを削除するための削除要求を前記第 1 保管サーバ装置に送信する処理を前記プロセッサに実行させる第 1 6 プログラムコードと

を備えたことを特徴とする記憶媒体。