(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-54363
(P2019-54363A)
(43)公開日　平成31年4月4日(2019.4.4)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08 (2006.01)		H04L	9/00	601A	5J104

審査請求 未請求　請求項の数 10　ＯＬ　（全 22 頁）

(21)出願番号　特願2017-176534 (P2017-176534)
(22)出願日　平成29年9月14日 (2017.9.14)

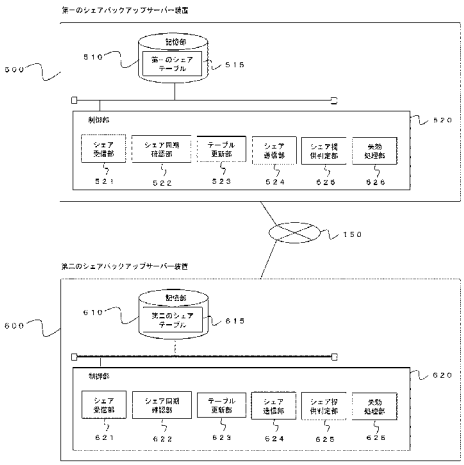
(71)出願人　000233491
株式会社日立システムズ
東京都品川区大崎一丁目２番１号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(72)発明者　壷内　将之
東京都品川区大崎１－２－１　株式会社日立システムズ内
(72)発明者　石井　健一
東京都品川区大崎１－２－１　株式会社日立システムズ内
(72)発明者　近野　雅樹
東京都品川区大崎１－２－１　株式会社日立システムズ内

最終頁に続く

(54)【発明の名称】サーバー装置、秘密分散管理システムおよび秘密分散管理装置

(57)【要約】　（修正有）
【課題】（ｋ，ｎ）閾値法による秘密分散管理において、ｎ個の分散鍵の記憶媒体を携行できない場合であっても、正当な利用者であれば秘密情報を安全に利用できる技術を提供する。
【解決手段】サーバー装置であって、記憶部と、シェア受信部と、テーブル更新部と、シェア送信部と、を備える。シェア受信部は、ネットワークを介して接続される秘密分散法により秘密分散管理を行う秘密分散管理装置から送信された秘密分散情報およびそのバージョンを特定する情報を受信する。テーブル更新部は、秘密分散情報およびバージョンを特定する情報を関連付けて記憶部に格納する。シェア送信部は、記憶部から秘密分散情報のうちバージョンが新しい情報と関連付けられた秘密分散情報を秘密分散管理装置へ送信する。
【選択図】図２

図2



【特許請求の範囲】
【請求項１】
記憶部と、シェア受信部と、テーブル更新部と、シェア送信部と、を備え、
前記シェア受信部は、ネットワークを介して接続される秘密分散法により秘密分散管理を行う秘密分散管理装置から送信された秘密分散情報およびそのバージョンを特定する情報を受信し、
前記テーブル更新部は、前記秘密分散情報および前記バージョンを特定する情報を関連付けて前記記憶部に格納し、
前記シェア送信部は、前記記憶部から前記秘密分散情報のうち前記バージョンが新しい情報と関連付けられた前記秘密分散情報を前記秘密分散管理装置へ送信する、
ことを特徴とするサーバー装置。
【請求項２】
請求項１に記載のサーバー装置であって、
前記テーブル更新部は、前記秘密分散情報の有効性を示す情報を前記秘密分散情報ごとに対応付けて格納し、
前記シェア送信部が前記秘密分散情報を前記秘密分散管理装置へ送信する際に、前記秘密分散情報の有効性を示す情報に応じて送信するか否かを判定するシェア提供判定部と、
を備えることを特徴とするサーバー装置。
【請求項３】
請求項２に記載のサーバー装置であって、
前記シェア提供判定部は、前記シェア送信部が前記秘密分散情報を前記秘密分散管理装置へ送信する際に、前記秘密分散情報が有効でない場合であって所定の特権ユーザーからの要求である場合には、前記秘密分散情報を送信する、
ことを特徴とするサーバー装置。
【請求項４】
サーバー装置と、該サーバー装置とネットワークを介して接続される秘密分散管理装置と、を含む秘密分散管理システムであって、
前記サーバー装置は、
記憶部と、シェア受信部と、テーブル更新部と、シェア送信部と、を備え、
前記シェア受信部は、前記秘密分散管理装置から送信されたシェアおよびそのバージョンを特定する情報を受信し、
前記テーブル更新部は、前記シェアおよび前記バージョンを特定する情報を関連付けて前記記憶部に格納し、
前記シェア送信部は、前記記憶部から前記シェアのうち前記バージョンが新しい情報と関連付けられた情報を前記秘密分散管理装置へ送信し、
前記秘密分散管理装置は、
秘密分散法を利用してデータセットを複数のシェアに分割しバージョンを特定する情報を生成し前記シェア各々を異なる管理単位の記憶領域に格納させるシェア生成部と、
ネットワークを介して接続される前記サーバー装置へ前記シェアの複製を各々送信するシェア送信部と、
前記記憶領域または前記サーバー装置から各々が格納するシェアを取得するシェア収集部と、
前記シェア収集部が取得したシェアを用いて前記データセットを復号する処理を行うシェア結合部と、
を備えることを特徴とする秘密分散管理システム。
【請求項５】
請求項４に記載の秘密分散管理システムであって、
前記サーバー装置では、
前記テーブル更新部は、前記シェアの有効性を示す情報を前記シェアごとに対応付けて格納し、

前記シェア送信部が前記シェアを前記秘密分散管理装置へ送信する際に、前記シェアの有効性を示す情報に応じて送信するか否かを判定するシェア提供判定部、
を備えることを特徴とする秘密分散管理システム。
【請求項６】
請求項５に記載の秘密分散管理システムであって、
前記サーバー装置では、
前記シェア提供判定部は、前記シェア送信部が前記シェアを前記秘密分散管理装置へ送信する際に、前記シェアが有効でない場合であって所定の特権ユーザーからの要求である場合には、前記シェアを送信する、
ことを特徴とする秘密分散管理システム。
【請求項７】
秘密分散法を利用してデータセットを複数のシェアに分割し、前記シェア各々を異なる管理単位の記憶領域に格納させるシェア生成部と、
ネットワークを介して接続される所定の複数のバックアップサーバーへ前記シェアの複製を各々送信するシェア送信部と、
前記記憶領域または前記バックアップサーバーから各々が格納するシェアを取得するシェア収集部と、
前記シェア収集部が取得したシェアを用いて前記データセットを復号する処理を行うシェア結合部と、
を備える秘密分散管理装置。
【請求項８】
請求項７に記載の秘密分散管理装置であって、
利用者の生体情報を取得する生体情報取得部と、
前記生体情報を用いた生体認証を行う生体情報照合部と、を備え、
前記シェア結合部は、前記生体情報照合部による認証に成功すると、前記データセットの復号を行う、
ことを特徴とする秘密分散管理装置。
【請求項９】
請求項７に記載の秘密分散管理装置であって、
前記シェア生成部は、前記記憶領域の一つとして、接続される所定のスマートフォンの記憶装置を用いる、
ことを特徴とする秘密分散管理装置。
【請求項１０】
請求項７に記載の秘密分散管理装置であって、
前記シェア生成部は、前記シェアごとにバージョン情報を付与し、
前記シェア結合部は、前記バージョン情報を用いてバージョンが整合するシェアを特定して前記データセットを復号する、
ことを特徴とする秘密分散管理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サーバー装置、秘密分散管理システムおよび秘密分散管理装置に関するものである。
【背景技術】
【０００２】
様々な情報システムにおいて、秘密情報の保護が求められているが、秘密情報の管理を厳重に行うと利用時に煩わしく、また利用に必要な情報の紛失や忘却により秘密情報へのアクセス手段が失われることが多い。例えば、（ｋ，ｎ）閾値法（ｋは自然数、ｎはｋより大きい自然数）に基づき生成されたｎ個の分散鍵（シェア）を活用することで、（ｎ－ｋ）個の分散鍵までのシェアを紛失しても復元できるが、利用者はｎ個の分散鍵の記憶媒

体を携行しなければならず、利便性が高いとはいえない。
【０００３】
特許文献１には、個人情報の利用を、自装置を保持する特定の利用者に限定する個人情報管理装置であって、暗号化された個人情報を記憶している情報記憶手段と、暗号化された個人情報の復号に用いられる復号鍵を用いて（ｋ，ｎ）閾値秘密分散法に基づき生成されたｎ個の分散鍵のうち、１の分散鍵を記憶している分散鍵記憶手段と、無線電波の到達距離が所定距離に制限されており、無線通信を行って、利用者の（ｎ－１）個の着用物品それぞれに重複なく付着された、１の分散鍵以外の（ｎ－１）個の分散鍵のいずれかを重複なく記憶している（ｎ－１）個の分散鍵記憶装置のそれぞれとリンクが確立できるか否かを確認するリンク確認手段と、（ｋ－１）個以上の分散鍵記憶装置とリンクが確立できている場合に、リンクが確立できている（ｋ－１）個の分散鍵記憶装置それぞれから分散鍵を取得する取得手段と、自装置が有する１の分散鍵と、（ｋ－１）個の分散鍵とから、（ｋ，ｎ）閾値秘密分散法に基づき復号鍵を復元し、（ｋ－１）個の分散鍵記憶装置とリンクが確立できている間のみ復号鍵を保持する復号鍵生成手段と、保持されている復号鍵を用いて、暗号化された個人情報を復号して保持し、（ｋ－１）個の分散鍵記憶装置とリンクが確立できなくなった場合には復号した個人情報を破棄する復号手段とを備える個人情報管理装置について記載されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特許第４７７１９４２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
上記技術は、（ｎ－ｋ）個までの分散鍵（シェア）を紛失しても復元できるが、（ｎ－ｋ）個を越えるシェアの紛失があった場合には、情報を復元することができない。
【０００６】
本発明の目的は、（ｋ，ｎ）閾値法による秘密分散管理において、（ｎ－ｋ）個を越えるシェアの紛失があった場合に、正当な利用者であれば秘密情報を安全に利用できる技術を提供することにある。
【課題を解決するための手段】
【０００７】
本願は、上記課題の少なくとも一部を解決する手段を複数含んでいるが、その例を挙げるならば、以下のとおりである。本発明の一態様に係るサーバー装置は、記憶部と、シェア受信部と、テーブル更新部と、シェア送信部と、を備え、上記シェア受信部は、ネットワークを介して接続される秘密分散法により秘密分散管理を行う秘密分散管理装置から送信された秘密分散情報およびそのバージョンを特定する情報を受信し、上記テーブル更新部は、上記秘密分散情報および上記バージョンを特定する情報を関連付けて上記記憶部に格納し、上記シェア送信部は、上記記憶部から上記秘密分散情報のうち上記バージョンが新しい情報と関連付けられた上記秘密分散情報を上記秘密分散管理装置へ送信する、ことを特徴とする。
【０００８】
また、上記のサーバー装置であって、上記テーブル更新部は、上記秘密分散情報の有効性を示す情報を上記秘密分散情報ごとに対応付けて格納し、上記シェア送信部が上記秘密分散情報を上記秘密分散管理装置へ送信する際に、上記秘密分散情報の有効性を示す情報に応じて送信するか否かを判定するシェア提供判定部と、を備えることを特徴とするものであってもよい。
【０００９】
また、上記のサーバー装置であって、上記シェア提供判定部は、上記シェア送信部が上記秘密分散情報を上記秘密分散管理装置へ送信する際に、上記秘密分散情報が有効でない

場合であって所定の特権ユーザーからの要求である場合には、上記秘密分散情報を送信する、ことを特徴とするものであってもよい。

【００１０】

また、本発明の別の態様にかかる秘密分散管理システムは、サーバー装置と、該サーバー装置とネットワークを介して接続される秘密分散管理装置と、を含む秘密分散管理システムであって、上記サーバー装置は、記憶部と、シェア受信部と、テーブル更新部と、シェア送信部と、を備え、上記シェア受信部は、上記秘密分散管理装置から送信されたシェアおよびそのバージョンを特定する情報を受信し、上記テーブル更新部は、上記シェアおよび上記バージョンを特定する情報を関連付けて上記記憶部に格納し、上記シェア送信部は、上記記憶部から上記シェアのうち上記バージョンが新しい情報と関連付けられた情報を上記秘密分散管理装置へ送信し、上記秘密分散管理装置は、秘密分散法を利用してデータセットを複数のシェアに分割しバージョンを特定する情報を生成し、上記シェア各々を異なる管理単位の記憶領域に格納させるシェア生成部と、ネットワークを介して接続される上記サーバー装置へ上記シェアの複製を各々送信するシェア送信部と、上記記憶領域または上記サーバー装置から各々が格納するシェアを取得するシェア収集部と、上記シェア収集部が取得したシェアを用いて上記データセットを復号する処理を行うシェア結合部と、を備えることを特徴とする。

【００１１】

また、上記の秘密分散管理システムであって、上記サーバー装置では、上記テーブル更新部は、上記秘密分散情報の有効性を示す情報を上記秘密分散情報ごとに対応付けて格納し、上記シェア送信部が上記秘密分散情報を上記秘密分散管理装置へ送信する際に、上記秘密分散情報の有効性を示す情報に応じて送信するか否かを判定するシェア提供判定部、を備えることを特徴とするものであってもよい。

【００１２】

また、上記の秘密分散管理システムであって、上記サーバー装置では、上記シェア提供判定部は、上記シェア送信部が上記秘密分散情報を上記秘密分散管理装置へ送信する際に、上記秘密分散情報が有効でない場合であって所定の特権ユーザーからの要求である場合には、上記秘密分散情報を送信する、ことを特徴とするものであってもよい。

【００１３】

また、本発明の別の態様にかかる秘密分散管理装置は、秘密分散法を利用してデータセットを複数のシェアに分割し、上記シェア各々を異なる管理単位の記憶領域に格納させるシェア生成部と、ネットワークを介して接続される所定の複数のバックアップサーバーへ上記シェアの複製を各々送信するシェア送信部と、上記記憶領域または上記バックアップサーバーから各々が格納するシェアを取得するシェア収集部と、上記シェア収集部が取得したシェアを用いて上記データセットを復号する処理を行うシェア結合部と、を備えることを特徴とする。

【００１４】

また、上記の秘密分散管理装置であって、利用者の生体情報を取得する生体情報取得部と、上記生体情報を用いた生体認証を行う生体照合部と、を備え、上記シェア結合部は、上記生体照合部による認証に成功すると、上記データセットの復号を行う、ことを特徴とするものであってもよい。

【００１５】

また、上記の秘密分散管理装置であって、上記シェア生成部は、上記記憶領域の一つとして、接続される所定のスマートフォンの記憶装置を用いる、ことを特徴とするものであってもよい。

【００１６】

また、上記の秘密分散管理装置であって、上記シェア生成部は、上記シェアごとにバージョン情報を付与し、上記シェア結合部は、上記バージョン情報を用いてバージョンが整合するシェアを特定して上記データセットを復号する、ことを特徴とするものであってもよい。

【発明の効果】
【００１７】
本発明によると、（ｋ，ｎ）閾値法による秘密分散管理において、（ｎ－ｋ）個を越えるシェアの紛失があった場合に、正当な利用者であれば秘密情報を安全に利用できる。
【００１８】
上記した以外の課題、構成および効果は、以下の実施形態の説明により明らかにされる。
【図面の簡単な説明】
【００１９】
【図１】実施形態に係る秘密分散管理システムのブロック図である。
【図２】シェアバックアップサーバー装置のブロック図である。
【図３】第一のシェアテーブルに格納されるデータ構造を示す図である。
【図４】第二のシェアテーブルに格納されるデータ構造を示す図である。
【図５】秘密分散管理装置のハードウェア構成例を示す図である。
【図６】生体情報読取装置のハードウェア構成例を示す図である。
【図７】シェアバックアップサーバー装置のハードウェア構成例を示す図である。
【図８】シェア生成処理のフローの例を示す図である。
【図９】シェアテーブル更新処理のフローの例を示す図である。
【図１０】データセット復元処理のフローの例を示す図である。
【発明を実施するための形態】
【００２０】
以下に、本発明の一態様に係る実施形態を適用した秘密分散管理システムを採用する業務システム１について、図面を参照して説明する。以下の実施の形態においては便宜上その必要があるときは、複数のセクションまたは実施の形態に分割して説明するが、特に明示した場合を除き、それらはお互いに無関係なものではなく、一方は他方の一部または全部の変形例、詳細、補足説明等の関係にある。
【００２１】
また、以下の実施の形態において、要素の数等（個数、数値、量、範囲等を含む）に言及する場合、特に明示した場合および原理的に明らかに特定の数に限定される場合等を除き、その特定の数に限定されるものではなく、特定の数以上でも以下でもよい。
【００２２】
さらに、以下の実施の形態において、その構成要素（要素ステップ等も含む）は、特に明示した場合および原理的に明らかに必須であると考えられる場合等を除き、必ずしも必須のものではないことは言うまでもない。
【００２３】
同様に、以下の実施の形態において、構成要素等の形状、位置関係等に言及するときは特に明示した場合および原理的に明らかにそうではないと考えられる場合等を除き、実質的にその形状等に近似または類似するもの等を含むものとする。このことは、上記数値および範囲についても同様である。
【００２４】
また、実施の形態を説明するための全図において、同一の部材には原則として同一の符号を付し、その繰り返しの説明は省略する。
【００２５】
図１は、本実施形態に係る秘密分散管理システムを備える業務システム１のブロック図である。業務システム１は、利用者１００が利用する秘密分散管理装置２００と、秘密分散管理装置２００に接続される外部記憶媒体３００と、秘密分散管理装置２００に接続される生体情報読取装置４００と、秘密分散管理装置２００とネットワーク１５０を介して通信可能な第一のシェアバックアップサーバー装置５００と、秘密分散管理装置２００とネットワーク１５０を介して通信可能な第二のシェアバックアップサーバー装置６００と、第一のシェアバックアップサーバー装置５００および第二のシェアバックアップサーバ

ー装置６００とネットワーク１５０を介して通信可能な特権ユーザー端末７００と、を含む。

【００２６】

ネットワーク１５０は、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）、インターネット、携帯電話網等、あるいはこれらが複合した通信網である。なお、ネットワーク１５０は、携帯電話通信網等の無線通信網上のＶＰＮ（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）等であってもよい。

【００２７】

業務システム１では、利用者が秘密分散管理装置２００を用いて入出力操作を行い、作成されたファイル等を含むデータセット（記憶部２２０の利用者が使用する記憶領域全体のデータであってもよいし、ファイル単位であってもよい）が秘密分散管理装置２００の記憶部２２０および外部記憶媒体３００に分散されたシェア（秘密情報の断片）の状態で格納される。また、秘密分散管理装置２００の記憶部２２０および外部記憶媒体３００に分散されたシェアは、第一のシェアバックアップサーバー装置５００および第二のシェアバックアップサーバー装置６００に、それぞれ格納される。

【００２８】

秘密分散管理装置２００は、シェアからデータセットを復元させる場合には、外部記憶媒体３００と、記憶部２２０とに格納されたシェアを利用して復号処理を行う。なお、その際、たとえば外部記憶媒体３００を紛失、あるいは利用時に利用者が携帯していない場合には、従来の技術では復号ができず、外部記憶媒体３００から第二のシェアを取得することができない。しかし、秘密分散管理装置２００は、ネットワーク１５０を介して第二のシェアバックアップサーバー装置６００から第二のシェアを取得することができる。そのため、（ｋ，ｎ）閾値法による秘密分散管理において、ｎ個の分散鍵の記憶媒体を携行できない場合、あるいは（ｎ－ｋ）個を越える分散鍵の紛失時でも、秘密情報を安全に利用できるといえる。

【００２９】

業務システム１の応用例を挙げると、業務システム１は、顧客情報等の個人情報の取り扱いを伴う業務システム、あるいは営業活動や経営資源にかかる社外秘情報の利用を伴う業務システム等がある。

【００３０】

その際には、利用者は、秘密分散管理装置２００を操作して、業務内容に応じて秘密を要する情報が含まれる文書ファイルや会計関連の情報が含まれる表計算ファイル（これらは、データセットであるといえる）を作成し、保存する。秘密分散管理装置２００は、このような文書ファイルや表計算ファイル等を含む秘密情報の保存処理において、秘密分散法を用いたシェアを複数作成して、秘密分散管理装置２００の記憶部２２０と、外部記憶媒体３００の記憶部３１０と、に分散させて管理する。なお、シェアのバックアップを、ネットワーク１５０を介して接続される第一のシェアバックアップサーバー装置５００および第二のシェアバックアップサーバー装置６００に保存することで、外部記憶媒体３００あるいは秘密分散管理装置２００の紛失時に復旧することができる。

【００３１】

また、利用者は、秘密分散管理装置２００を操作して、上記のように分散管理の対象となる文書ファイルや表計算ファイルにアクセスする際には、秘密分散管理装置２００は、分散管理された同じバージョンのシェアを集めて復号し、データセットを復元させることができる。

【００３２】

なお、そのようなデータセットの復元処理においては、その途中で生体情報を照合して利用者の生体認証を行うこともできる。秘密分散管理装置２００は、生体認証により正当な利用者であること、あるいは特権ユーザーによるログインが確認された場合に復元処理を完了させる。

【００３３】

その他には、秘密分散管理システムを備える業務システム１では、パーソナルコンピュータ向け秘密分散ソフト単体での使用と比較して、電子ファイルをネットワークを介してバックアップするため、シェア格納媒体を紛失したり、秘密分散管理装置２００がマルウェアに感染したりしても、電子ファイルの復元が可能である点が優れている。また、シェアを紛失しても元の電子ファイルを復元できるシェアの個数に対する、携行するシェアの個数が少なくて済む(例えば、１個までのシェアが漏洩しても元の電子ファイルの漏洩を防ぎ（ｋ＞１）、２個までのシェアを紛失しても元の電子ファイルを復元可能とするためには、（１，２)閾値法で十分となり、利用者は2個の媒体を携行するだけでよい）。また、複数のサーバー装置にシェアを保存するため、バックアップの通信経路のうち１つを盗聴されても、元の電子ファイルが漏洩しない。そのため、バックアップに用いる通信経路をＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）等で強固に保護する必要がなくなり、システムの安価な運用が可能となる。また、シェアの結合に失敗した際や、シェアを紛失した際に、自動的にバックアップサーバー装置からシェアをダウンロードする構成にすることで、シームレスに元の電子ファイルを復元することが可能となる。

【００３４】

外部記憶媒体３００は、例えばＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）メモリーや、ＳＤカード等の記憶媒体、スマートフォンを含む記憶領域を備える電子装置またはその他の電子記憶媒体である。また、外部記憶媒体３００と秘密分散管理装置２００との接続は、例えばＵＳＢ接続、Ｂｌｕｅｔｏｏｔｈ（登録商標）接続、ＮＦＣ（Ｎｅａｒ　Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ）接続、２．５４ＧＨｚ帯の無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等の各種の接続が可能である。

【００３５】

生体情報読取装置４００は、利用者１００の生体情報を読み取る装置である。例えば、生体情報読取装置４００は、利用者１００の指紋、声紋、虹彩、静脈等のいずれかの生体情報を読み取り、秘密分散管理装置２００へ受け渡す。また、生体情報読取装置４００と秘密分散管理装置２００との接続は、例えばＵＳＢ接続、Ｂｌｕｅｔｏｏｔｈ（登録商標）接続、ＮＦＣ（Ｎｅａｒ　Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ）接続、２．５４ＧＨｚ帯の無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等の各種の接続が可能である。

【００３６】

第一のシェアバックアップサーバー装置５００は、いわゆるサーバー装置等の情報処理装置であり、秘密分散管理装置２００、第二のシェアバックアップサーバー装置６００および特権ユーザー端末７００との接続は、ネットワーク１５０を介して接続される。第二のシェアバックアップサーバー装置６００についても、同様である。

【００３７】

特権ユーザー端末７００は、いわゆるパソコン等の情報処理装置であり、秘密分散管理装置２００、第一のシェアバックアップサーバー装置５００および第二のシェアバックアップサーバー装置６００との接続は、ネットワーク１５０を介して接続される。

【００３８】

秘密分散管理装置２００は、業務システム１の利用者を認証することができる情報処理装置である。秘密分散管理装置２００は、制御部２１０と、記憶部２２０と、通信部２３０と、入力部２４０と、出力部２５０と、を備える。制御部２１０には、シェア生成部２１１と、シェア結合部２１２と、シェア送信部２１３と、シェア収集部２１４と、生体情報照合部２１５と、が含まれる。

【００３９】

シェア生成部２１１は、秘密分散法を利用してデータセットを複数のシェアに分割する。具体的には、シェア生成部２１１は、記憶部２２０の所定の記憶領域（データセット）について、（ｋ，ｎ）閾値法によりシェア（秘密分散情報）を生成する。その際、シェア生成部２１１は、シェアごとにバージョン情報を付与する。また、シェア生成部２１１は、生成したシェアにバージョン情報を対応付けて、シェアごとに異なる管理単位の記憶領

域（例えば、相互に動作に影響を与えない秘密分散管理装置２００の記憶部２２０と、外部記憶媒体３００の記憶部３１０と）に格納させる。

【００４０】

シェア結合部２１２は、シェア収集部２１４が取得したシェアを用いてデータセットを復号する処理を行う。具体的には、シェア結合部２１２は、シェア収集部２１４が取得したシェアのバージョンが整合するものを組み合わせて、復号処理を行い、データセットの復元を行う。また、そのデータセットを記憶部２２０あるいはメモリの所定の領域に仮想領域として展開する。

【００４１】

シェア送信部２１３は、ネットワーク１５０を介して接続される第一のシェアバックアップサーバー装置５００およびネットワーク１５０を介して接続される第二のシェアバックアップサーバー装置６００へシェアの複製を各々送信する。具体的には、シェア送信部２１３は、第一のシェアバックアップサーバー装置５００に第一のシェアを送信し、第二のシェアバックアップサーバー装置６００に第二のシェアを送信する。これらのシェアとシェアの送信先のシェアバックアップサーバー装置とは、あらかじめ対応付けられている。

【００４２】

シェア収集部２１４は、秘密分散管理装置２００の記憶部２２０および外部記憶媒体３００の記憶部３１０、またはシェアバックアップサーバー装置から、各々が格納するシェアを取得する。

【００４３】

生体情報照合部２１５は、秘密分散されたデータセットの復元時に、所定の生体認証処理を行い、正当な利用者であることの確認および特権ユーザーであるか否かの判定を行う。

【００４４】

なお、生体情報照合部２１５は、記憶部２２０の生体情報テンプレート２２１にあらかじめ格納されている利用者の生体情報と、認証の要求時に受け渡された利用者１００の生体情報と、を用いて所定のアルゴリズムで生体情報のマッチングを行い、所定以上の一致度を有する場合には認証成功と判定し、そうでない場合には認証失敗と判定する。ただし、生体認証の処理はこれに限られるものではない。

【００４５】

記憶部２２０には、生体情報テンプレート２２１と、第一のシェア２２２と、が格納される。生体情報テンプレート２２１は、生体情報照合部２１５による生体情報の照合による利用者の特定、特権ユーザーであるか否かの判定に用いられる情報である。第一のシェア２２２には、記憶部２２０あるいはメモリに展開されたデータセットから生成したシェアのうち一部の断片が格納される。

【００４６】

通信部２３０は、ネットワーク１５０を介して他の装置である第一のシェアバックアップサーバー装置５００、第二のシェアバックアップサーバー装置６００および特権ユーザー端末７００との通信を行う。

【００４７】

入力部２４０は、秘密分散管理装置２００への利用者１００からの入力を受け付ける。例えば、入力部２４０は、タイピングやタッチ、フリック入力等の各種の接触入力、あるいは音声入力、または視線入力等の各種の入力を受け付ける。

【００４８】

出力部２５０は、秘密分散管理装置２００からの利用者１００への出力を行う。出力される情報は、画面や帳票等の各種出力情報である。

【００４９】

外部記憶媒体３００は、記憶部３１０を備える。記憶部３１０には、第二のシェア３１５が格納される。第二のシェア３１５には、秘密分散管理装置２００の記憶部２２０ある

いはメモリに展開されたデータセットから生成したシェアのうち一部の断片が格納される。

【００５０】

生体情報読取装置４００は、生体情報取得部４１０を備える。生体情報取得部４１０は、指示を受けると、所定の生体情報の読み取りを行い、秘密分散管理装置２００へ読み取った生体情報を受け渡す。

【００５１】

図２は、シェアバックアップサーバー装置のブロック図である。本実施形態においては、シェアバックアップサーバー装置としては、第一のシェアバックアップサーバー装置５００と、第二のシェアバックアップサーバー装置６００と、が備えられるが、これに限られるものではなく、少なくとも独立した２つ以上のシェアバックアップサーバー装置が備えられていればよい。

【００５２】

第一のシェアバックアップサーバー装置５００には、記憶部５１０と、制御部５２０と、が含まれる。記憶部５１０には、第一のシェアテーブル５１５が含まれる。制御部５２０には、シェア受信部５２１と、シェア同期確認部５２２と、テーブル更新部５２３と、シェア送信部５２４と、シェア提供判定部５２５と、失効処理部５２６と、が含まれる。

【００５３】

図３は、第一のシェアテーブルに格納されるデータ構造を示す図である。第一のシェアテーブル５１５には、複数の秘密分散管理装置２００のシェアが、秘密分散管理装置２００およびバージョンごとに格納される。第一のシェアテーブル５１５には、端末ＩＤ５１５Ａと、失効５１５Ｂと、シェアのバージョン５１５Ｃと、更新日時５１５Ｄと、シェアバイナリデータ５１５Ｅと、が対応付けて格納される。端末ＩＤ５１５Ａは、秘密分散管理装置２００を特定する情報である。失効５１５Ｂは、端末が失効している、すなわち端末ＤＩ５１５Ａで特定される秘密分散管理装置２００からのアクセスが禁止されているか否かを特定する情報である。シェアのバージョン５１５Ｃは、シェアのバージョンを特定する情報である。更新日時５１５Ｄは、シェアが格納された日時を特定する情報である。シェアバイナリデータ５１５Ｅは、シェアのバイナリデータである。

【００５４】

シェア受信部５２１は、秘密分散管理装置２００からシェアを受信する。シェア同期確認部５２２は、受信したシェアが、他のシェアバックアップサーバー装置と同期されているか否か確認する。具体的には、シェア同期確認部５２２は、テーブル更新部５２３により第一のシェアテーブル５１５の更新がなされると、他のシェアバックアップサーバー装置へ端末ＩＤとバージョン情報を送信し、一致することを確認する。一致しない場合には、シェア同期確認部５２２は、テーブル更新部５２３に更新を取り消しさせる。あるいは、シェア同期確認部５２２は、他のシェアバックアップサーバー装置から端末ＩＤとバージョン情報が送信されると、受信したシェアの端末ＩＤとバージョン情報に一致することを確認する。一致しない場合には、他のシェアバックアップサーバー装置へその旨を通知する。

【００５５】

テーブル更新部５２３は、シェア受信部５２１が受信したシェアを用いて、第一のシェアテーブル５１５を更新する。なお、バージョン管理を行うほうが望ましいため、テーブル更新部５２３は、レコード追加により第一のシェアテーブル５１５を更新するが、これに限られるものではなく、以前のバージョンのシェアを削除して新たなシェアを格納するようにしてもよい。

【００５６】

シェア送信部５２４は、第一のシェアテーブル５１５に格納されたシェアのうち、端末ＩＤで識別される秘密分散管理装置２００ごとに最新のバージョンあるいは指定されたバージョンのシェアを読み出し、当該秘密分散管理装置２００へ送信する。

【００５７】

シェア提供判定部５２５は、シェア送信部５２４がシェアを送信する際に、シェアの有効性を示す情報に応じて送信するか否かを判定する。シェアの有効性を示す情報は、失効５１５Ｂ、アクセスした端末ＩＤおよびユーザーＩＤにより特定される。シェア提供判定部５２５は、いずれかのバージョンのシェアについて、失効５１５Ｂが「１」に設定されている秘密分散管理装置２００からのシェアの要求に対しては、シェアを送信しない。ただし、特権ユーザー端末７００を用いて特権ユーザーが要求している場合には、この限りではなく、特権ユーザー端末７００へ最新のシェアを送信する。

【００５８】

失効処理部５２６は、秘密分散管理装置２００あるいは外部記憶媒体３００の紛失時等、シェアを転得者（第三者）から取得されるのを防ぐ処理を行う。具体的には、失効処理部５２６は、特権ユーザー端末７００からの特権ユーザーによるアクセスに応じて、失効させるべき端末ＩＤを受け付けて、当該端末ＩＤのすべてのバージョンのシェアについて、第一のシェアテーブル５１５の失効５１５Ｂと、第二のシェアテーブル６１５の失効６１５Ｂとに、有効でないことを意味する「１」を設定する。逆に、紛失が解消した場合には、失効処理部５２６は、特権ユーザー端末７００からの特権ユーザーによるアクセスに応じて、有効にすべき端末ＩＤを受け付けて、第二のシェアバックアップサーバー装置６００から最新バージョンのシェアを取得してデータセットを復元する。そして、失効処理部５２６は、シェア生成部２１１と同様の秘密分散法を利用してデータセットを複数のシェアに分割する。その際、失効処理部５２６は、古いバージョンとシェアを一致させないために、乱数等を用いて異なるシェアを生成する。また、失効処理部５２６は、シェアを各シェアバックアップサーバー装置へ失効していない情報として格納させる。そして、失効処理部５２６は、特権ユーザー端末７００へすべてのシェアを受け渡す。

【００５９】

第二のシェアバックアップサーバー装置６００には、記憶部６１０と、制御部６２０と、が含まれる。記憶部６１０には、第二のシェアテーブル６１５が含まれる。制御部６２０には、シェア受信部６２１と、シェア同期確認部６２２と、テーブル更新部６２３と、シェア送信部６２４と、シェア提供判定部６２５と、失効処理部６２６と、が含まれる。

【００６０】

図４は、第二のシェアテーブルに格納されるデータ構造を示す図である。第二のシェアテーブル６１５には、複数の秘密分散管理装置２００のシェアが、秘密分散管理装置２００およびバージョンごとに格納される。第二のシェアテーブル６１５には、端末ＩＤ６１５Ａと、失効６１５Ｂと、シェアのバージョン６１５Ｃと、更新日時６１５Ｄと、シェアバイナリデータ６１５Ｅと、が対応付けて格納される。端末ＩＤ６１５Ａは、秘密分散管理装置２００を特定する情報である。失効６１５Ｂは、端末が失効している、すなわち端末ＩＤ６１５Ａで特定される秘密分散管理装置２００からのアクセスが禁止されているか否かを特定する情報である。シェアのバージョン６１５Ｃは、シェアのバージョンを特定する情報である。更新日時６１５Ｄは、シェアが格納された日時を特定する情報である。シェアバイナリデータ６１５Ｅは、シェアのバイナリデータである。

【００６１】

シェア受信部６２１は、秘密分散管理装置２００からシェアを受信する。シェア同期確認部６２２は、受信したシェアが、他のシェアバックアップサーバー装置と同期されているか否か確認する。具体的には、シェア同期確認部６２２は、テーブル更新部６２３により第二のシェアテーブル６１５の更新がなされると、他のシェアバックアップサーバー装置へ端末ＩＤとバージョン情報を送信し、一致することを確認する。一致しない場合には、シェア同期確認部６２２は、テーブル更新部５２３に更新を取り消しさせる。あるいは、シェア同期確認部６２２は、他のシェアバックアップサーバー装置から端末ＩＤとバージョン情報が送信されると、受信したシェアの端末ＩＤとバージョン情報に一致することを確認する。一致しない場合には、他のシェアバックアップサーバー装置へその旨を通知する。

【００６２】

テーブル更新部６２３は、シェア受信部６２１が受信したシェアを用いて、第二のシェアテーブル６１５を更新する。なお、バージョン管理を行うほうが望ましいため、テーブル更新部６２３は、レコード追加により第二のシェアテーブル６１５を更新するが、これに限られるものではなく、以前のバージョンのシェアを削除して新たなシェアを格納するようにしてもよい。

【００６３】

シェア送信部６２４は、第二のシェアテーブル６１５に格納されたシェアのうち、端末ＩＤで識別される秘密分散管理装置２００ごとに最新のバージョンあるいは指定されたバージョンのシェアを読み出し、当該秘密分散管理装置２００へ送信する。

【００６４】

シェア提供判定部６２５は、シェア送信部６２４がシェアを送信する際に、シェアの有効性を示す情報に応じて送信するか否かを判定する。シェアの有効性を示す情報は、失効６１５Ｂ、アクセスした端末ＩＤおよびユーザーＩＤにより特定される。シェア提供判定部６２５は、いずれかのバージョンのシェアについて、失効６１５Ｂが「１」に設定されている秘密分散管理装置２００からのシェアの要求に対しては、シェアを送信しない。ただし、特権ユーザー端末７００を用いて特権ユーザーが要求している場合には、この限りではなく、特権ユーザー端末７００へ最新のシェアを送信する。

【００６５】

失効処理部６２６は、秘密分散管理装置２００あるいは外部記憶媒体３００の紛失時等、シェアを転得者（第三者）から取得されるのを防ぐ処理を行う。具体的には、失効処理部６２６は、特権ユーザー端末７００からの特権ユーザーによるアクセスに応じて、失効させるべき端末ＩＤを受け付けて、当該端末ＩＤの最新バージョンのシェアについて、第二のシェアテーブル６１５の失効６１５Ｂに、有効でないことを意味する「１」を設定する。逆に、紛失が解消した場合には、失効処理部６２６は、特権ユーザー端末７００からの特権ユーザーによるアクセスに応じて、有効にすべき端末ＩＤを受け付けて、当該端末ＩＤのすべてのバージョンのシェアについて、第二のシェアテーブル６１５の失効６１５Ｂに、有効を意味する「０」を設定する。

【００６６】

図１の説明に戻る。特権ユーザー端末７００は、シェアの管理を行う特権を有するユーザーが使用する端末である。例えば、秘密分散管理装置２００あるいは外部記憶媒体３００等のシェアの紛失時に、利用者１００から連絡を受けてシェアの利用を制限したり、新たな秘密分散管理装置２００の利用を始めた利用者１００に対して、直前のバージョンのシェアの取得および提供（データ復旧）を行うための端末である。特権ユーザー端末７００は、他の秘密分散管理装置２００と同様の構成を備える。

【００６７】

図５は、秘密分散管理装置のハードウェア構成例を示す図である。秘密分散管理装置２００は、いわゆるパーソナルコンピュータあるいはタブレット端末の筐体により実現されるハードウェア構成を備える。秘密分散管理装置２００は、演算装置２０１と、主記憶装置２０２と、補助記憶装置２０３と、通信装置２０４と、外部記憶媒体接続装置２０５と、生体情報読取装置接続装置２０６と、各装置をつなぐバス２０７と、を備える。また他に、秘密分散管理装置２００は、タッチパネルやキーボード、マイク、ディスプレイ等の入出力装置を備える。

【００６８】

演算装置２０１は、例えばＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）などの演算装置である。

【００６９】

主記憶装置２０２は、例えばＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）などのメモリ装置である。

【００７０】

補助記憶装置２０３は、デジタル情報を記憶可能な、いわゆるハードディスク（Ｈａｒ

ｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）やＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）あるいはフラッシュメモリなどの不揮発性記憶装置である。

【００７１】

通信装置２０４は、ネットワーク１５０等を介して第一のシェアバックアップサーバー装置５００、第二のシェアバックアップサーバー装置６００、等の他の装置と通信経路を確立し、情報を送受信するネットワークカード等の装置である。

【００７２】

外部記憶媒体接続装置２０５は、ＵＳＢメモリやスマートフォンと接続するためのＵＳＢインターフェースを備える。生体情報読取装置接続装置２０６は、ＵＳＢインターフェースを備える。

【００７３】

なお、入出力装置には、キーボードやマウス、タッチパネル、ディスプレイ、マイク、スピーカー等の各種入出力装置が含まれる。

【００７４】

入出力装置と、演算装置２０１と、主記憶装置２０２と、補助記憶装置２０３と、通信装置２０４と、外部記憶媒体接続装置２０５と、生体情報読取装置接続装置２０６とは、バス２０７等の接続導線により互いに接続される。

【００７５】

上記した秘密分散管理装置２００のシェア生成部２１１と、シェア結合部２１２と、シェア送信部２１３と、シェア収集部２１４と、生体情報照合部２１５とは、演算装置２０１に処理を行わせるプログラムによって実現される。このプログラムは、主記憶装置２０２、補助記憶装置２０３または図示しないＲＯＭ装置内に記憶され、実行にあたって主記憶装置２０２上にロードされ、演算装置２０１により実行される。

【００７６】

また、秘密分散管理装置２００の記憶部２２０は、主記憶装置２０２及び補助記憶装置２０３により実現される。また、秘密分散管理装置２００の通信部２３０は、通信装置２０４により実現される。入力部２４０および出力部２５０は、入出力装置により実現される。以上が、秘密分散管理装置２００のハードウェア構成例である。

【００７７】

図６は、生体情報読取装置のハードウェア構成例を示す図である。生体情報読取装置４００は、生体情報取得装置４０１と、演算装置４０２と、主記憶装置４０３と、外部接続装置４０４と、各装置をつなぐバス４０５と、を備える。

【００７８】

生体情報取得装置４０１は、指紋、静脈紋、虹彩、声紋等、生体の情報を取得するためのユニットであり、その取得情報に応じて、赤外線リーダー、カメラ、マイク等各種の入力装置を備える。

【００７９】

演算装置４０２は、例えばＣＰＵなどの演算装置である。

【００８０】

主記憶装置４０３は、例えばＲＡＭなどのメモリ装置である。

【００８１】

外部接続装置４０４は、ＵＳＢにより秘密分散管理装置２００への接続を行う装置である。

【００８２】

上記した生体情報読取装置４００の生体情報取得部４１０は、演算装置４０２に処理を行わせるプログラムによって実現される。このプログラムは、主記憶装置４０３または図示しないＲＯＭ装置内に記憶され、実行にあたって主記憶装置４０３上にロードされ、演算装置４０２により実行される。以上が、生体情報読取装置４００のハードウェア構成例である。

【００８３】

図７は、シェアバックアップサーバー装置のハードウェア構成例を示す図である。第一のシェアバックアップサーバー装置５００および第二のシェアバックアップサーバー装置６００は、いわゆるパーソナルコンピュータあるいはタブレット端末の筐体により実現されるハードウェア構成を備える。第一のシェアバックアップサーバー装置５００は、演算装置５０１と、主記憶装置５０２と、補助記憶装置５０３と、通信装置５０４と、各装置をつなぐバス５０５と、を備える。なお、第二のシェアバックアップサーバー装置６００についても、第一のシェアバックアップサーバー装置５００と略同様のハードウェア構成を備えるため、説明を省略する。

【００８４】

演算装置５０１は、例えばＣＰＵなどの演算装置である。

【００８５】

主記憶装置５０２は、例えばＲＡＭなどのメモリ装置である。

【００８６】

補助記憶装置５０３は、デジタル情報を記憶可能な、いわゆるハードディスクやＳＳＤあるいはフラッシュメモリなどの不揮発性記憶装置である。

【００８７】

通信装置５０４は、ネットワーク１５０等を介して他のシェアバックアップサーバー装置、特権ユーザー端末７００、秘密分散管理装置２００等の他の装置と通信経路を確立し、情報を送受信するネットワークカード等の装置である。

【００８８】

演算装置５０１と、主記憶装置５０２と、補助記憶装置５０３と、通信装置５０４とは、バス５０５等の接続導線により互いに接続される。

【００８９】

上記した第一のシェアバックアップサーバー装置５００のシェア受信部５２１と、シェア同期確認部５２２と、テーブル更新部５２３と、シェア送信部５２４と、シェア提供判定部５２５とは、演算装置５０１に処理を行わせるプログラムによって実現される。このプログラムは、主記憶装置５０２、補助記憶装置５０３または図示しないＲＯＭ装置内に記憶され、実行にあたって主記憶装置５０２上にロードされ、演算装置５０１により実行される。

【００９０】

また、第一のシェアバックアップサーバー装置５００の記憶部５１０は、主記憶装置５０２及び補助記憶装置５０３により実現される。また、図示しない通信部は、通信装置５０４により実現される。以上が、第一のシェアバックアップサーバー装置５００のハードウェア構成例である。

【００９１】

秘密分散管理装置２００、第一のシェアバックアップサーバー装置５００および第二のシェアバックアップサーバー装置６００のそれぞれの構成は、処理内容に応じて、さらに多くの構成要素に分類することもできる。また、１つの構成要素がさらに多くの処理を実行するように分類することもできる。

【００９２】

また、各制御部（シェア生成部２１１と、シェア結合部２１２と、シェア送信部２１３と、シェア収集部２１４と、生体情報照合部２１５と、シェア受信部５２１と、シェア同期確認部５２２と、テーブル更新部５２３と、シェア送信部５２４と、シェア提供判定部５２５）は、それぞれの機能を実現する専用のハードウェア（ＡＳＩＣ、ＧＰＵなど）により構築されてもよい。また、各制御部の処理が一つのハードウェアで実行されてもよいし、複数のハードウェアで実行されてもよい。

【００９３】

次に、本実施形態における業務システム１の動作を説明する。

【００９４】

図８は、シェア生成処理のフローの例を示す図である。シェア生成処理は、秘密分散管

理装置２００の終了処理、あるいはスタンバイ等の休眠状態への移行時に起動される。
【００９５】
まず、シェア生成部２１１は、メモリあるいは記憶部２２０に展開されている仮想領域を対象として、シェアを生成し、所定の記憶部にシェアを保存する（ステップＳ２００）。具体的には、シェア生成部２１１は、従来技術の所定のアルゴリズムを用いてシェアを生成し、バージョンを自動付番し、バージョン、端末ＩＤとともに記憶部２２０および外部記憶媒体３００の記憶部３１０にそれぞれ第一のシェア２２２、第二のシェア３１５を格納する。
【００９６】
そして、シェア送信部２１３は、第一のシェアと、バージョンと、端末ＩＤとを第一のシェアバックアップサーバー装置５００へ送信する（ステップＳ２１０）。また、シェア送信部２１３は、第二のシェアと、バージョンと、端末ＩＤとを第二のシェアバックアップサーバー装置６００へ送信する（ステップＳ２１１）
【００９７】
第一のシェアバックアップサーバー装置５００のシェア受信部５２１は、第一のシェアと、バージョンと、端末ＩＤとを受信する（ステップＳ２２０）。また、第二のシェアバックアップサーバー装置６００のシェア受信部６２１は、第二のシェアと、バージョンと、端末ＩＤとを受信する（ステップＳ２２１）。
【００９８】
そして、第一のシェアバックアップサーバー装置５００のシェア同期確認部５２２は、第二のシェアバックアップサーバー装置６００へ、同期確認のために、受信した第一のシェアのバージョンと、端末ＩＤとを送信する（ステップＳ２３０）。
【００９９】
そして、第二のシェアバックアップサーバー装置６００のシェア同期確認部６２２は、受信した第二のシェアのバージョンおよび端末ＩＤと、第一のシェアバックアップサーバー装置５００から受信した第一のシェアのバージョンと端末ＩＤと、を比較し、一致するか否かを第一のシェアバックアップサーバー装置５００へ送信する（ステップＳ２３１）。
【０１００】
そして、第一のシェアバックアップサーバー装置５００のシェア同期確認部５２２は、一致する旨の情報を受信した場合には受信完了（ＹＥＳ）として、一致しない場合（ＮＯ）には再送要求を秘密分散管理装置２００へ送信する（ステップＳ２４０）。再送要求がなされると（ステップＳ２４０で「ＮＯ」の場合）、秘密分散管理装置２００のシェア送信部２１３は、第一のシェアと第二のシェアを再送するために、制御をステップＳ２１０へ戻す。
【０１０１】
受信完了の場合（ステップＳ２４０にて「ＹＥＳ」の場合）には、第一のシェアバックアップサーバー装置５００のテーブル更新部５２３は、第一のシェアテーブル５１５を更新する（ステップＳ２５０）。具体的には、テーブル更新部５２３は、受信した端末ＩＤを端末ＩＤ５１５Ａに格納し、失効５１５Ｂに有効を示す初期値「０」を格納し、受信したバージョンをシェアのバージョン５１５Ｃに格納し、処理時点の日時を更新日時５１５Ｄに格納し、受信したシェアをシェアバイナリデータ５１５Ｅに格納する。
【０１０２】
また、受信完了の場合（ステップＳ２４０にて「ＹＥＳ」の場合）には、第二のシェアバックアップサーバー装置６００のテーブル更新部６２３は、第二のシェアテーブル６１５を更新する（ステップＳ２５１）。具体的には、テーブル更新部６２３は、受信した端末ＩＤを端末ＩＤ６１５Ａに格納し、失効６１５Ｂに有効を示す初期値「０」を格納し、受信したバージョンをシェアのバージョン６１５Ｃに格納し、処理時点の日時を更新日時６１５Ｄに格納し、受信したシェアをシェアバイナリデータ６１５Ｅに格納する。
【０１０３】

そして、第一のシェアバックアップサーバー装置５００のテーブル更新部５２３および第二のシェアバックアップサーバー装置６００のテーブル更新部６２３は、更新完了を秘密分散管理装置２００へ通知する。

【０１０４】

秘密分散管理装置２００のシェア送信部２１３は、メモリあるいは記憶部２２０に展開されている仮想領域を削除することで、シェア生成の元となったデータセットを秘密分散管理装置２００上から取り除く（ステップＳ２６０）。

【０１０５】

以上が、シェア生成処理の流れである。シェア生成処理によれば、秘密分散管理装置２００の仮想領域上で生成された秘密情報等のデータセットがすべて（ｋ，ｎ）閾値法によりシェアとして分割され、記憶部２２０の第一のシェア２２２と記憶部３１０の第二のシェア３１５として保存される。そのため、データセットはシェアを復号しない限り復元できなくなる。また、シェアのバックアップをサーバー装置上に有するため、媒体の紛失時等においても、データセットの復元を行うための元データとなるシェアが失われて復元不能となることを避けられる。

【０１０６】

図９は、シェアテーブル更新処理のフローの例を示す図である。シェアテーブル更新処理は、シェア生成処理のステップＳ２５０、ステップＳ２５１において実施される。

【０１０７】

まず、第一のシェアバックアップサーバー装置５００においては、シェア受信部５２１が第一のシェアの受信を完了すると（ステップＳ３００）、テーブル更新部５２３が受信したシェアを第一のシェアテーブル５１５に追加する（ステップＳ３１０）。この際の処理は、上述のステップＳ２５０のとおりである。

【０１０８】

そして、テーブル更新部５２３は、所定の削除条件（例えば、３世代以前のバージョンは削除）を読み取り、第一のシェアテーブル５１５から削除対象のシェアのエントリを削除する（ステップＳ３２０）。

【０１０９】

同様に、第二のシェアバックアップサーバー装置６００においては、シェア受信部６２１が第二のシェアの受信を完了すると（ステップＳ４００）、テーブル更新部６２３が受信したシェアを第二のシェアテーブル６１５に追加する（ステップＳ４１０）。この際の処理は、上述のステップＳ２５１のとおりである。

【０１１０】

そして、テーブル更新部６２３は、所定の削除条件（例えば、３世代以前のバージョンは削除）を読み取り、第二のシェアテーブル６１５から削除対象のシェアのエントリを削除する（ステップＳ４２０）。

【０１１１】

以上が、シェアテーブル更新処理の流れである。シェアテーブル更新処理によれば、最新のシェアをシェアテーブルに格納するとともに、所定以上古いバージョンのシェアを削除して、シェアテーブルの肥大化を避けることができる。

【０１１２】

図１０は、データセット復元処理のフローの例を示す図である。データセット復元処理は、秘密分散管理装置２００の起動時、あるいは休止状態からの復帰時に開始される。

【０１１３】

まず、シェア収集部２１４は、第一のシェア２２２およびそのバージョン情報と、第二のシェア３１５およびそのバージョン情報とを、それぞれ記憶部２２０と記憶部３１０とから取得する（ステップＳ１００）。

【０１１４】

そして、シェア結合部２１２は、バージョンを確認する（ステップＳ１１０）。具体的には、シェア結合部２１２は、ステップＳ１００において取得した第一のシェア２２２と

第二のシェア３１５のバージョン情報が一致するか否か判定する。
【０１１５】
バージョン情報が一致する場合（ステップＳ１１０にて「ＹＥＳ」の場合）には、生体情報照合部２１５は、利用者認証を行う（ステップＳ１２０）。具体的には、生体情報照合部２１５は、生体情報読取装置４００の生体情報取得部４１０に指示して生体情報を取得し、記憶部２２０の生体情報テンプレート２２１との一定以上の一致度を有する場合には利用認証を行い、そうでない場合には利用認証を行わない。
【０１１６】
利用認証を行った場合（ステップＳ１２０にて「ＹＥＳ」の場合）には、シェア結合部２１２は、第一のシェアと第二のシェアとを用いて復号し、データセットを復元させ、メモリあるいは記憶部２２０の仮想記憶領域に展開する（ステップＳ１３０）。そして、データセット復元処理を終了させる。
【０１１７】
利用認証を行わなかった場合（ステップＳ１２０にて「ＮＯ」の場合）には、シェア結合部２１２は、起動失敗と判定する（ステップＳ１８０）。シェア結合部２１２は、利用者に対し、運用スタッフに連絡する旨のメッセージを表示する等の処理を行う。そして、データセット復元処理を終了させる。
【０１１８】
バージョン情報が一致しない場合（ステップＳ１１０にて「ＮＯ」の場合）には、シェア収集部２１４は、第一のシェアバックアップサーバー装置５００と第二のシェアバックアップサーバー装置６００との通信の接続を確認する（ステップＳ１４０）。いずれかのシェアバックアップサーバー装置との通信が失敗する場合には、シェア結合部２１２は、起動失敗と判定する（ステップＳ１８０）。シェア結合部２１２は、利用者に対し、運用スタッフに連絡する旨のメッセージを表示する等の処理を行う。そして、データセット復元処理を終了させる。
【０１１９】
そして、シェア収集部２１４は、第一のシェアバックアップサーバー装置５００あるいは第二のシェアバックアップサーバー装置６００に、シェアのダウンロードを要求する（ステップＳ１５０）。具体的には、シェア収集部２１４は、ステップＳ１００にて取得した第一のシェア２２２、第二のシェア３１５のうち、新しいバージョンを有するシェアに対応するバージョンの他のシェアのダウンロード要求を第一のシェアバックアップサーバー装置５００あるいは第二のシェアバックアップサーバー装置６００に送信する。ここで、シェア収集部２１４は、シェアに不足がある場合には、存在するシェアのバージョンを新しいバージョンのシェアとし、そのバージョンと合致する他のシェアのダウンロード要求を送信する。
【０１２０】
そして、第一のシェアバックアップサーバー装置５００のシェア提供判定部５２５あるいは第二のシェアバックアップサーバー装置６００のシェア提供判定部６２５は、ダウンロード要求で指定されたバージョンのシェアが存在するかどうかを、第一のシェアテーブル５１５あるいは第二のシェアテーブル６１５に問い合わせる（ステップＳ１６０、Ｓ１７０）。存在した場合、シェア提供判定部５２５あるいはシェア提供判定部６２５は、該当するシェアを要求した秘密分散管理装置２００の端末ＩＤについて、失効とされているか否かを判定する。失効でない場合には、シェア送信部５２４あるいはシェア送信部６２４は、秘密分散管理装置２００に送信する。シェアが存在しなかった場合、あるいは失効している端末ＩＤである場合には、シェア送信部５２４あるいはシェア送信部６２４は、その旨を秘密分散管理装置２００に送信し、起動失敗処理（ステップＳ１８０）に移る。
【０１２１】
なお、特権ユーザーがシェアの要求を行っている場合には、シェア提供判定部５２５あるいはシェア提供判定部６２５は、該当するシェアを要求した秘密分散管理装置２００の端末ＩＤについて失効とされている場合であっても、シェア送信部５２４あるいはシェア

送信部６２４に対して、秘密分散管理装置２００あるいは特権ユーザー端末７００にシェアを送信させる。

【０１２２】

以上が、データセット復元処理の流れである。データセット復元処理によれば、まずは秘密分散管理装置２００の記憶部２２０および外部記憶媒体の記憶部３１０からシェアを取得してデータセットを復元することができる。適切なシェアが取得できない場合であっても、ネットワーク１５０を介してバックアップされたシェアを取得してデータセットを復元することができる。また、紛失等の事態が発生した場合には、データセットを復元するためのダウンロードを制限することができ、その場合であっても特権ユーザーからの要求であれば、ネットワーク１５０を介してバックアップされたシェアを取得してデータセットを復元することができる。

【０１２３】

以上が、本発明の実施形態にかかる業務システム１である。業務システム１によれば、（ｋ，ｎ）閾値法による秘密分散管理において、（ｎ－ｋ）個を越えるシェアの紛失があった場合に、正当な利用者であれば秘密情報を安全に利用できる

【０１２４】

本発明は、上記の実施形態に制限されない。上記の実施形態は、本発明の技術的思想の範囲内で様々な変形が可能である。例えば、上記の実施形態においては、利用認証は予め定められた生体認証を用いる例が示されているが、これに限られない。例えば、ワンタイムパスワード等、他のパスワード認証であってもよい。あるいは、ＳＮＳ（Ｓｏｃｉａｌ Ｎｅｔｗｏｒｋｉｎｇ Ｓｅｒｖｉｃｅ）等の他の情報システムで登録されているアカウントを利用するものとすることもできる。

【０１２５】

また、上記した実施形態の技術的要素は、単独で適用されてもよいし、プログラム部品とハードウェア部品のような複数の部分に分けられて適用されるようにしてもよい。

【０１２６】

以上、本発明について、実施形態を中心に説明した。

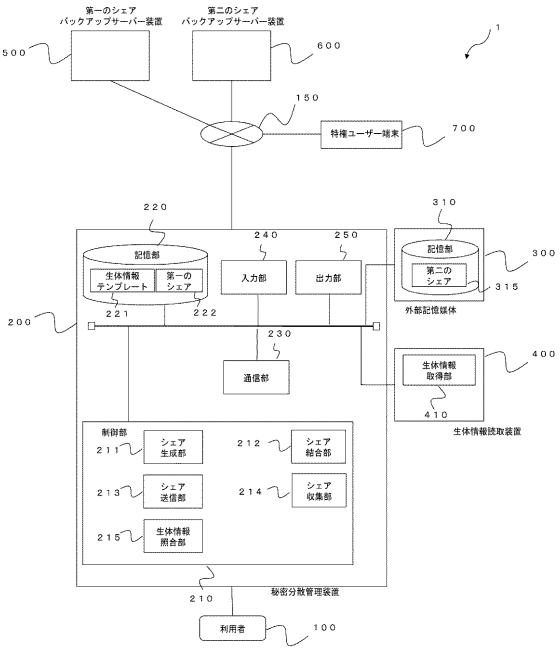
【符号の説明】

【０１２７】

１・・・業務システム、１００・・・利用者、１５０・・・ネットワーク、２００・・・秘密分散管理装置、２１０・・・制御部、２１１・・・シェア生成部、２１２・・・シェア結合部、２１３・・・シェア送信部、２１４・・・シェア収集部、２１５・・・生体情報照合部、２２０・・・記憶部、２２１・・・生体情報テンプレート、２２２・・・第一のシェア、２３０・・・通信部、２４０・・・入力部、２５０・・・出力部、３００・・・外部記憶媒体、３１０・・・記憶部、３１５・・・第二のシェア、４００・・・生体情報読取装置、４１０・・・生体情報取得部、５００・・・第一のシェアバックアップサーバー装置、６００・・・第二のシェアバックアップサーバー装置、７００・・・特権ユーザー端末

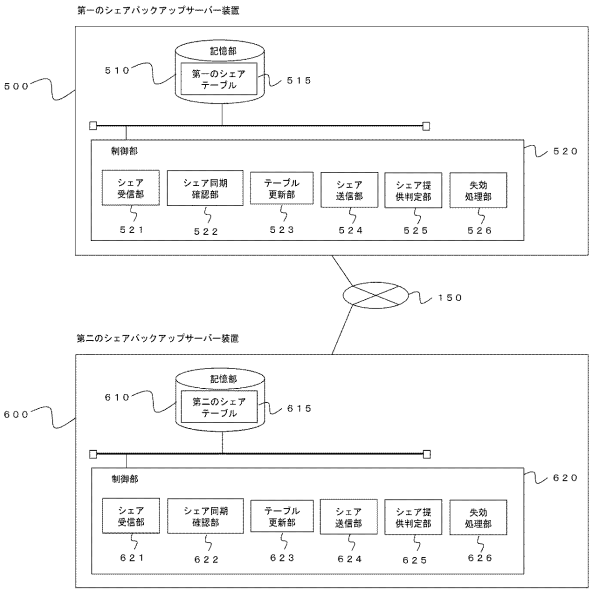
【図１】

図1



【図２】

図2



【図３】

図3

第一のシェアテーブル515

515A 端末ID	515B 失効	515C シェアのバージョン	515D 更新日時	515E シェアバイナリデータ	･･
00123456	0	5	2017/6/23 11:54	CB00D814A568DFA0･･･	･･
00123456	0	6	2017/6/24 17:27	12CB6E58AF8DD576･･･	･･
00123456	1	7	2017/6/25 19:12	BB1E1E69633F1A9C･･･	･･
98765432	0	2	2017/6/12 16:45	B622C45028299B6A･･･	･･
98765432	0	3	2017/6/18 20:21	8643A74EF44BE4E1･･･	･･
:	:	:	:	:	･･
:	:	:	:	:	･･

【図４】

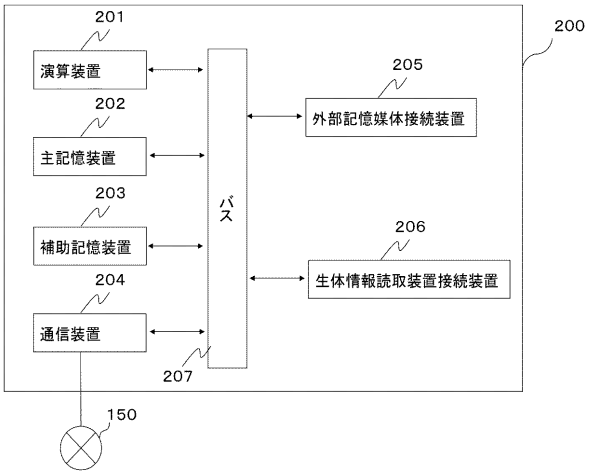
図4

第二のシェアテーブル615

615A 端末ID	615B 失効	615C シェアのバージョン	615D 更新日時	615E シェアバイナリデータ	･･
00123456	0	5	2017/6/23 11:54	34DB75AC004B9863･･･	･･
00123456	0	6	2017/6/24 17:27	51E68D67AB342153･･･	･･
00123456	1	7	2017/6/25 19:12	23456789ABCDEF01･･･	･･
98765432	0	2	2017/6/12 16:45	77FB80381C459DDF･･･	･･
98765432	0	3	2017/6/18 20:21	6448DFD9F4F6E9D3･･･	･･
:	:	:	:	:	･･
:	:	:	:	:	･･

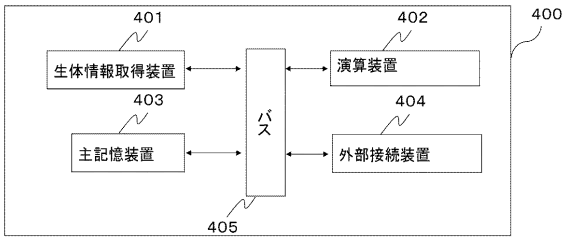
【図５】

図5



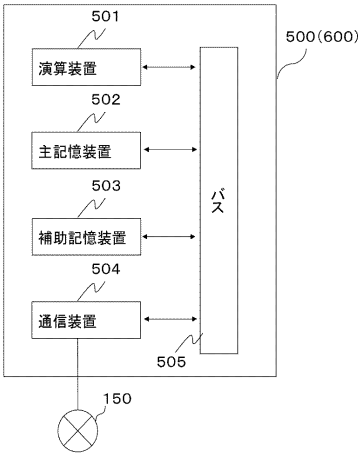
【図６】

図6



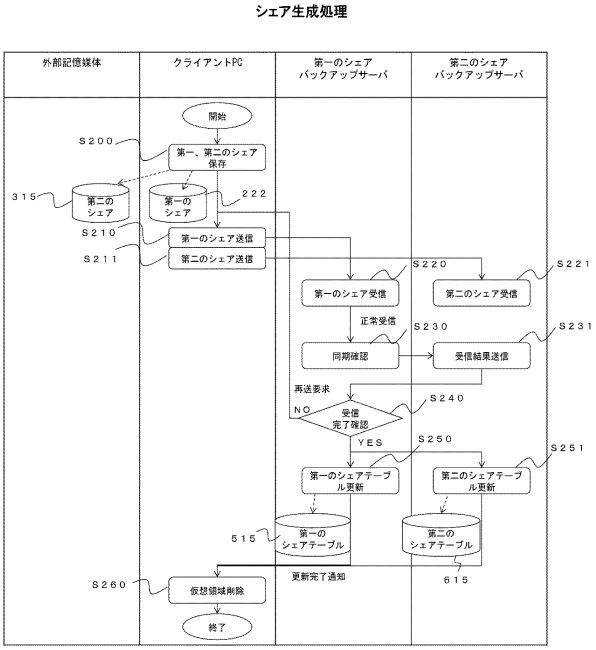
【図７】

図7



【図８】

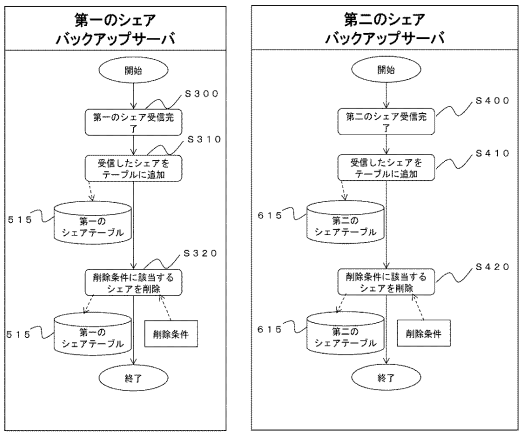
図8



【図９】

図9

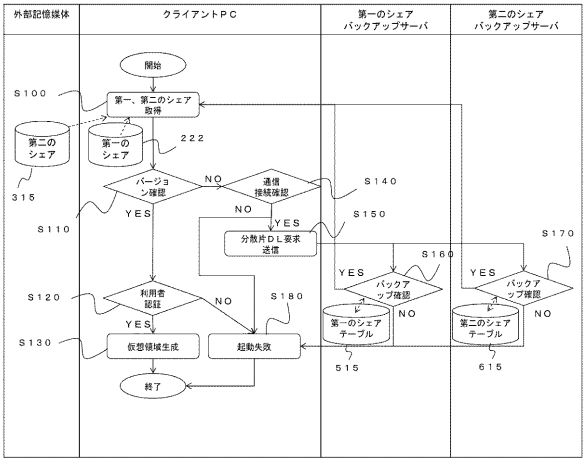
シェアテーブル更新処理



【図１０】

図10

データセット復元処理



フロントページの続き

(72)発明者　▲高▼村　啓輝
東京都品川区大崎１－２－１　株式会社日立システムズ内

Ｆターム(参考) 5J104 AA07 AA16 EA02 EA04 EA08 EA13 EA16 KA01 KA16 NA02
PA07