(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第4875781号
(P4875781)
(45)発行日　平成24年2月15日(2012.2.15)　(24)登録日　平成23年12月2日(2011.12.2)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 12/14 510F

請求項の数 7 (全 18 頁)

(21)出願番号　特願2011-151338(P2011-151338)
(22)出願日　平成23年7月8日(2011.7.8)
審査請求日　平成23年7月8日(2011.7.8)

早期審査対象出願

(73)特許権者　000155469
株式会社野村総合研究所
東京都千代田区丸の内一丁目６番５号
(74)代理人　100080001
弁理士　筒井　大和
(74)代理人　100093023
弁理士　小塚　善高
(74)代理人　100117008
弁理士　筒井　章子
(72)発明者　新谷　敏文
東京都港区東新橋一丁目５番２号　汐留シティセンター　エヌ・アール・アイ・セキュアテクノロジーズ株式会社内

最終頁に続く

(54)【発明の名称】データ分散保管システム

(57)【特許請求の範囲】
【請求項１】
クライアント端末において、重要データから秘密分散技術により複数の非重要データである部分データを生成し、前記各部分データを、ネットワークを介して接続された複数のサーバに分散保管するデータ分散保管システムであって、
前記各サーバは、それぞれ、前記クライアント端末から受信した前記部分データを保管するデータ保管部を有し、
前記クライアント端末は、ユーザから保管を指示された前記重要データから前記秘密分散技術によりｋ個以上集めなければ前記重要データを復元できないｎ個（ｋ≦ｎ）の前記部分データを生成する分割処理部と、
前記分割処理部によって生成されたｎ個の前記部分データ、および前記各部分データのｎ個のコピーを、２ｎ個以上の前記サーバの中から、保管する前記重要データ毎に順次ローテーションさせて選択した２ｎ個の前記サーバの前記データ保管部にそれぞれ保管し、また、前記重要データを復元するためのｍ個（ｋ≦ｍ≦ｎ）の異なる前記部分データもしくは前記部分データのコピーをｍ個の前記サーバからそれぞれ収集する分散管理部と、
前記ユーザから利用を指示された前記重要データについて、前記分散管理部から取得したｍ個の異なる前記部分データもしくは前記部分データのコピーから前記秘密分散技術により前記重要データを復元する復元処理部とを有することを特徴とするデータ分散保管システム。
【請求項２】

請求項１に記載のデータ分散保管システムにおいて、
前記各サーバは、さらに、前記サーバへのアクセスに対しての認証処理を行う認証処理部を有し、
前記クライアント端末は、さらに、前記分散管理部が前記各サーバに対して前記部分データもしくは前記部分データのコピーを保管する際、および前記各サーバから前記部分データもしくは前記部分データのコピーを収集する際に、前記ユーザからユーザＩＤおよびパスワードの指定を受けて前記各サーバに対して順次もしくは並行的に認証の要求を送信する認証要求部を有し、
前記サーバの前記認証処理部は、前記サーバ毎に異なる固有情報であるサーバシーズと、登録されたユーザのユーザＩＤ毎に、前記ユーザ毎に異なる固有情報であるユーザシーズと、前記ユーザのパスワードを前記サーバシーズおよび前記ユーザシーズを用いて所定の手順でハッシュ化したハッシュ化パスワードとを含むアカウント情報を保持するユーザ情報とを有し、前記クライアント端末から受信した前記認証の要求に対して、前記サーバシーズと対象の前記ユーザに係る前記ユーザシーズ、および生成した乱数を前記クライアント端末に対して送信し、
前記クライアント端末の前記認証要求部は、前記ユーザから指定されたパスワードを、前記サーバから受信した前記サーバシーズおよび前記ユーザシーズを用いて所定の手順でハッシュ化し、さらに前記乱数を用いてハッシュ化したハッシュ値を前記サーバに送信し、
前記サーバの前記認証処理部は、前記クライアント端末から受信した前記ハッシュ値と、対象の前記ユーザに係る前記ハッシュ化パスワードを前記乱数を用いてハッシュ化した値とを比較して認証を行い、認証結果を前記クライアント端末に送信することを特徴とするデータ分散保管システム。
【請求項３】
請求項２に記載のデータ分散保管システムにおいて、
さらに、前記ネットワークに接続され、前記各サーバからの要求に基づいて、前記各サーバに対して前記シーズとなるシード値を生成して提供するマスタサーバを有することを特徴とするデータ分散保管システム。
【請求項４】
請求項１～３のいずれか１項に記載のデータ分散保管システムにおいて、
前記クライアント端末の前記分散管理部は、ｎ個の前記部分データおよび前記各部分データのｎ個のコピーを２ｎ個の前記サーバにそれぞれ保管した際に、前記各部分データおよび前記各部分データのコピーがいずれの前記サーバに保管されているかの対応に係る情報を分散状況記録部に記録することを特徴とするデータ分散保管システム。
【請求項５】
請求項１～４のいずれか１項に記載のデータ分散保管システムにおいて、
前記クライアント端末は、前記秘密分散技術に係るｋ、ｍ、ｎの値、前記各サーバに対するアクセス情報、前記分散管理部がｎ個の前記部分データおよび前記各部分データのｎ個のコピーを保管する対象となる２ｎ個の前記サーバを選択する条件、前記分散管理部がｍ個の異なる前記部分データもしくは前記部分データのコピーを収集する対象となるｍ個の前記サーバを選択する条件、および前記分散管理部が前記サーバから前記部分データもしくは前記部分データのコピーを取得できなかった場合の代替となる前記サーバの決定方法のうち、少なくとも１つ以上の情報が予め設定された設定情報を有することを特徴とするデータ分散保管システム。
【請求項６】
請求項１～５のいずれか１項に記載のデータ分散保管システムにおいて、
前記クライアント端末の前記分散管理部は、ｎ個の前記部分データおよび前記各部分データのｎ個のコピーを２ｎ個の前記サーバにそれぞれ保管する際に、ｎ個の前記部分データのいずれかと当該部分データのコピーの双方とも前記サーバに保管できなかった場合、もしくはｍ個の異なる前記部分データもしくは前記部分データのコピーを前記サーバから

それぞれ収集する際に、ｋ個以上収集できなかった場合は、前記ユーザに対してエラーを応答することを特徴とするデータ分散保管システム。

【請求項７】

請求項１～６のいずれか１項に記載のデータ分散保管システムにおいて、

前記クライアント端末および前記各サーバは、前記部分データもしくは前記部分データのコピーを送受信する際に、送信する前記部分データもしくは前記部分データのコピーを所定の手段で暗号化することを特徴とするデータ分散保管システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、電子データの保管技術に関し、特に、重要データから秘密分散技術により複数の非重要データを生成して複数の拠点に分散保管するデータ分散保管システムに適用して有効な技術に関するものである。

【背景技術】

【０００２】

情報システムを有する企業等においては、情報漏洩などの情報セキュリティ事故を防止するため、機密性の高いデータなどの重要なデータを保護する手段を講じる必要がある。一方でこれらを実現するための様々な手段も提案されている。

【０００３】

重要データを保護するための手段として、例えば、企業等が重要データをセキュリティ対策が多重に施されたデータセンターに保管することが考えられる。しかしながら、外部からアクセス可能なプライベートなデータセンターを独自に構築・運用するのは技術面・コスト面等で多大な負荷を要し、容易に実現できるものではない。

【０００４】

これに対して第三者が運用してサービスとして外部に提供しているデータセンターを利用することも考えられる。しかし、第三者が運用管理するデータセンターに自社の重要データを保管することはセキュリティ面で高いリスクが伴う。ましてや近年利用が拡大しているクラウドコンピューティング環境における仮想データセンターや仮想サーバに重要データを保管することは非常にリスクが高いことから、重要データを取り扱う業務を行う情報システムをクラウドコンピューティング環境を利用して構築するということがなかなか普及しない一因ともなっている。

【０００５】

一方、重要データを保管する際に、データを秘匿化したり改竄を防止したりする手段を講じて保管することも行われている。一般的には、暗号鍵を用いて重要データを暗号化して保管することが行われているが、この場合、暗号化されたデータには重要データの情報が全て含まれている。従って、例えば暗号化データが第三者に取得されたような場合、何らかの理由で当該第三者に暗号鍵も取得、解読された場合は容易に重要データが復元されてしまう。また、暗号鍵を取得されなくとも、暗号鍵が有限長であることから、理論上は有限回数の試行によって暗号化されたデータから重要データが復元されてしまう可能性を有する。

【０００６】

これに対し、重要データを強固に秘匿化する手法として、いわゆる秘密分散の技術も用いられている。秘密分散では、重要データを、それだけでは意味のない（重要データを復元・推測できない）非重要データに分割・分散することで、一部の非重要データが第三者に取得された場合でも、第三者による重要データの復元を理論上も不可能とすることができる。

【０００７】

秘密分散の手法としては種々のものが提案されている。例えば、特許第４０３９８１０号明細書（特許文献１）には、電子情報ファイルを複数の情報エレメントに分割し、分割された情報エレメントを選択し順序を変えて組み合わせることにより、２個以上の情報ブ

ロックであって全ての情報ブロックを統合しなければ全ての情報エレメントを含むことにならないような情報ブロックを生成し、情報エレメントに分割した方法に係る分割情報と情報ブロックを生成した方法に係る形成情報を記録した分割抽出データを生成し、各情報ブロックと分割抽出データとのうち、少なくとも１つを証明局に保管し、他を分離して別々に保管することで電子情報の安全を確保する技術が開示されている。

【０００８】

一方、重要データに対応する非重要データや情報ブロック（以下では“部分データ”と記載する場合がある）を全て集めなくとも所定の個数以上集めれば重要データを復元可能な秘密分散の手法として、例えば、非特許文献１に記載されたような多項式補間を用いた（ｋ，ｎ）閾値秘密分散法が従来から用いられている。この手法によれば、ｎ個に分散した部分データのうち少なくともｋ個（ｋ≦ｎ）を集めれば重要データを復元することができる。また、この手法をさらに改良した種々の閾値秘密分散法も提案されている。

【０００９】

これに関連して、例えば、特開２００９－１３９９９０号公報（特許文献２）には、記憶装置に格納されたデータを、復元の際に基準個数の部分データが必要となる秘密分散法により、基準個数以上の所定の個数の部分データに分割する分割部と、部分データを他の情報処理装置に送信するとともに記憶装置から削除する送信部と、記憶装置へデータを復元する場合に、他の情報処理装置から部分データを取得して記憶装置に格納する取得部と、基準個数の部分データが記憶装置に格納されたことを条件にデータを復元する復元部とを備える情報処理装置が開示されている。

【先行技術文献】

【特許文献】

【００１０】

【特許文献１】特許第４０３９８１０号明細書

【特許文献２】特開２００９－１３９９９０号公報

【非特許文献】

【００１１】

【非特許文献１】A.Shamir、"How to Share a Secret"、Communications of the ACM、vol.22 no.11 pp.612-613、1979.

【発明の概要】

【発明が解決しようとする課題】

【００１２】

近年、ノート型ＰＣ（Personal Computer）などの携帯可能な情報処理端末が広く利用されるに従って、これらの端末自体の盗難や紛失等に伴う情報漏洩のリスクが高まっている。例えば、個人情報等を取り扱う企業などにおいては、従業員等がこれらの端末を紛失したような場合には、監督官庁への届出や報告等が必要となる場合がある。しかし、従来は実際の情報漏洩範囲については特定することができない場合がほとんどであり、紛失した時点で全てのデータが漏洩もしくはその可能性があると報告せざるを得なかった。

【００１３】

これに対して、端末内の重要データを含むデータを外部のサーバ等に保管することで端末の紛失等に伴う情報漏洩のリスクを低減することが考えられる。このとき、重要データをそのまま外部のサーバ等に保管するのではなく、例えば、上述した秘密分散の技術を利用して重要データを非重要データに分割・分散して部分データとし、これを外部のサーバ等に分散保管するようにすることで、例えば、クラウドコンピューティング環境における仮想データセンターや仮想サーバなどに保管するような場合においても情報漏洩のリスクを低減させることが可能である。

【００１４】

すなわち、各データセンター等に分散保管される部分データは、それ自体では意味をなさず、当該部分データのみからは重要データの内容を復元したり推測したりすることができない。従って、当該データセンターやサーバ等に不正に侵入し、当該部分データを取得

した第三者はもちろん、例えば、各データセンターの管理者等の内部の者が悪意を持って当該部分データを取得した場合でも、取得された部分データから重要データの内容が漏洩する事態を防ぐことができる。

【００１５】

また、秘密分散の技術により重要データを複数の部分データに分割・分散した場合、部分データの一部が滅失した場合でも、所定の個数以上の部分データを集めることができれば元の重要データを復元できることから、データの可用性を向上させることもできる。例えば、（ｋ，ｎ）閾値型の秘密分散により、重要データからｎ個の部分データを生成した場合、ｋ個以上の部分データを集めることができれば重要データを復元することができる。換言すれば、（ｎ－ｋ）個までの部分データの滅失には耐えることが可能である。

【００１６】

しかしながら、現実の情報システムの実装において、重要データのセキュアな取り扱いが必要とされる場面では、暗号化の技術が広く一般に用いられているのと比較して、上述した秘密分散の技術は未だあまり適用されていないのが現状である。このため、現時点では、利用実績や処理速度等の観点で、実用に耐え得る機能や性能を有する秘密分散のライブラリは限られている。

【００１７】

これらのライブラリでは、例えば、秘密分散に係る機能が固定化されていたり、制約があったり等、秘密分散によって得られる可用性を拡張・変更することができないことが多く、データの可用性が、使用する秘密分散のライブラリの機能や仕様に依存してしまうという状況となっている。

【００１８】

そこで本発明の目的は、重要データから秘密分散技術により生成された複数の部分データを複数のデータセンターに分散保管するにあたり、秘密分散を実装するライブラリ等の機能もしくは仕様に依存せずにデータの可用性を向上させることができるデータ分散保管システムを提供することにある。

【００１９】

本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

【課題を解決するための手段】

【００２０】

本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、以下のとおりである。

【００２１】

本発明の代表的な実施の形態によるデータ分散保管システムは、クライアント端末において、重要データから秘密分散技術により複数の非重要データである部分データを生成し、前記各部分データを、ネットワークを介して接続された複数のサーバに分散保管するデータ分散保管システムであって、以下の特徴を有するものである。

【００２２】

すなわち、前記各サーバは、それぞれ、前記クライアント端末から受信した前記部分データを保管するデータ保管部を有する。

【００２３】

また、前記クライアント端末は、ユーザから保管を指示された前記重要データから前記秘密分散技術によりｋ個以上集めなければ前記重要データを復元できないｎ個（ｋ≦ｎ）の前記部分データを生成する分割処理部と、前記分割処理部によって生成されたｎ個の前記部分データ、および前記各部分データのｎ個のコピーを、２ｎ個の前記サーバの前記データ保管部にそれぞれ保管し、また、前記重要データを復元するためのｍ個（ｋ≦ｍ≦ｎ）の異なる前記部分データもしくは前記部分データのコピーをｍ個の前記サーバからそれぞれ収集する分散管理部と、前記ユーザから利用を指示された前記重要データについて、前記分散管理部から取得したｍ個の異なる前記部分データもしくは前記部分データのコピ

ーから前記秘密分散技術により前記重要データを復元する復元処理部とを有する。
【発明の効果】
【００２４】
本願において開示される発明のうち、代表的なものによって得られる効果を簡単に説明すれば以下のとおりである。
【００２５】
本発明の代表的な実施の形態によれば、重要データから秘密分散技術により生成された複数の部分データを複数のデータセンターに分散保管するにあたり、秘密分散を実装するライブラリ等の機能もしくは仕様に依存せずにデータの可用性を向上させることが可能となる。
【図面の簡単な説明】
【００２６】
【図１】本発明の一実施の形態であるデータ分散保管システムの構成例について概要を示した図である。
【図２】本発明の一実施の形態におけるデータの保管の概念について説明した図である。
【図３】本発明の一実施の形態におけるデータの可用性の例について説明した図である。
【図４】本発明の一実施の形態におけるデータの可用性の別の例について説明した図である。
【図５】本発明の一実施の形態における部分データを保管するサーバの選択の例について示した図である。
【図６】本発明の一実施の形態における認証処理の流れの例について概要を示した図である。
【発明を実施するための形態】
【００２７】
以下、本発明の実施の形態を図面に基づいて詳細に説明する。なお、実施の形態を説明するための全図において、同一部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。
【００２８】
＜概要＞
本発明の一実施の形態であるデータ分散保管システムは、ユーザがクライアント端末上で、ユーザの重要データを保管する際に、当該重要データから秘密分散技術により複数の部分データを生成し、これらを複数のデータセンターのサーバに送信して分散保管する。このとき、各部分データのコピーをそれぞれ別のデータセンターに保管して二重化する。これにより、後述するように、使用する秘密分散のライブラリの機能や仕様に依存せず、データの可用性を大きく向上させることができる。
【００２９】
また、各データセンターに対するシングルサインオンの仕組みを実装し、認証の際に、各データセンターで異なる固有情報（鍵）を用いて認証処理を行うことで、各データセンターへのアクセスを独立して安全に行えるようにし、各データセンター間でのセキュリティを確保する。これらにより、各データセンターの管理者等の内部の者であっても１つの部分データしか得ることができず、当該部分データから重要データを復元・推測することはできないため、ユーザは安全に重要データを保管することができる。
【００３０】
図２は、本実施の形態のデータ分散保管システムにおけるデータの保管の概念について説明した図である。データ分散保管システム１は、クライアント端末３００と、複数のデータセンター１０（図２の例では１０ａ～ｈの８つ）が図示しないネットワークを介して接続された構成を有している。ここで、クライアント端末３００は、ユーザが業務等で通常使用し、重要データ５００の入力や参照などの処理を行う情報処理端末であり、例えば、ＰＣや、タブレット型端末、スマートフォン、携帯電話などの携帯端末などが該当する。

【００３１】
また、データセンター１０は、サーバ機器を保管して運用管理を行う拠点であり、例えば、多数のサーバ機器等を保管して高度な運用管理を行うことができる専用のデータセンター施設や、いわゆるコンテナ型やモジュール型などの可搬型のデータセンターなどであってもよいし、オフィスビル内のマシンルームなど専用ではない施設であってもよい。また、クラウドコンピューティング環境における仮想データセンターであってもよい。本実施の形態での各データセンター１０は、それぞれ、データを保持・記憶するためのストレージ機器等からなるデータ保管部１１０（図２の例では１１０ａ～１１０ｈ）を有するサーバ（図示しない）を１台以上有している。
【００３２】
なお、これらの各データセンター１０は、地理的にも組織的にも相互に関連のないものとするのが望ましい。すなわち、例えば同一の敷地内や隣接する敷地に存在したり、同一もしくは関連する事業者等により運用されていたりなど、データセンター１０間で、管理者等が相互に物理的もしくは電子的にアクセスすることが可能な構成とはなっていないものとするのが望ましい。
【００３３】
上記のような環境で、ユーザからの指示に基づいて、クライアント端末３００に存在する重要データ５００についてセキュアな保管を行う場合、まず、クライアント端末３００において、重要データ５００から秘密分散技術を利用して複数の部分データ５１０（図２の例では５１０ａ～５１０ｄの４つ）を生成する。それぞれの部分データ５１０は、上述したように、単独では意味をなさない非重要データである。なお、重要データ５００は漏洩を防止するために削除する。
【００３４】
利用する秘密分散技術（秘密分散のアルゴリズム）については特に限定されず、例えば、ｎ個の部分データ５１０うちｋ個以上集めれば重要データ５００を復元することができるが、ｋ個未満では原則として重要データ５００を復元することができない、いわゆる（ｋ，ｎ）閾値型（１＜ｋ≦ｎ）の秘密分散の手法を用いることができる。また、ｋ、ｎの値も特に限定されず、セキュリティの強度や可用性、処理速度等の要件などに応じて適宜決定することができる。なお、ｎの値（生成する部分データ５１０の数）はデータセンター１０の数の半分以下であるものとする。換言すれば、ｎ個の部分データ５１０（図２の例では４つ）に対して２ｎ個以上のデータセンター１０（図２の例では８つ）が利用可能となるようにする。
【００３５】
生成した４つの部分データ５１０は、それぞれコピーを作成して二重化し、図示するように、重複しないように８つのデータセンター１０に振り分けて送信し、データ保管部１１０に分散保管する。すなわち、同一の重要データ５００から生成した部分データ５１０（以下では、特に断らない限り部分データ５１０にはコピーも含むものとする）は、それぞれ別個に異なるデータセンター１０に保管するものとし、いずれか２つ以上の部分データ５１０が同一のデータセンター１０に保管されることがないようにする。なお、クライアント端末３００上の各部分データ５１０は漏洩を防止するために削除する。
【００３６】
以上のように、重要データ５００から秘密分散技術により部分データ５１０を生成して各データセンター１０に分散保管することで、クライアント端末３００の盗難や紛失等による重要データ５００の漏洩を防止することができる。また、各データセンター１０は重要データ５００につき部分データ５１０を１つしか有していないため、データセンター１０に対して第三者が侵入して不正に部分データ５１０を取得したり、データセンター１０の管理者等の内部の者が部分データ５１０を取得したりした場合でも、部分データ５１０を１つしか得ることができない。当該部分データ５１０だけでは重要データ５００を復元・推測することはできないため、重要データ５００の内容が漏洩することはない。
【００３７】

また、各データセンター１０が地理的にも組織的にも相互に関連のないものとなっている場合には、データセンター１０の管理者等の内部の者が、他のデータセンター１０にアクセスすることも、後述する認証処理と合わせて、困難である。従って、例えば、データセンター１０の管理者等の内部の者が悪意を持った場合でも、他のデータセンター１０から部分データ５１０を不正に取得し、ｋ個以上集めて重要データ５００を復元してしまうという事態を防止することができる。

【００３８】

また、各部分データ５１０をそれぞれ異なるデータセンター１０に保管して二重化することで、使用する秘密分散のライブラリの機能や仕様に依存せず、通常データの単なるバックアップの場合と比較して、リソースの必要量に対するデータの可用性を大きく向上させることができる。

【００３９】

例えば、重要データ５００から（３，４）閾値型の秘密分散により４つの部分データ５１０を生成し、これらを４つのデータセンター１０にそれぞれ分散保管した場合、そのうちの３つの部分データ５１０を集めることができれば、元の重要データ５００を復元することができる。すなわち、１つのデータセンター１０での障害等による部分データ５１０の滅失等には耐えることができる。これに対し、上述の図２の例に示したように、４つの部分データ５１０およびそれらのコピーを、８つの異なるデータセンター１０にそれぞれ分散保管することにより、リソースの必要量の増加分に比して、全体としてデータの可用性を大きく向上させることができる。

【００４０】

図３および図４は、本実施の形態のデータ分散保管システムにおけるデータの可用性の例について説明した図である。図３の例では、図２の例に示したように、部分データ５１０を８つのデータセンター１０に二重化して分散保管している状態で、５つのデータセンター１０ａ、ｃ、ｄ、ｆ、ｈにおいて障害等により部分データ５１０が取得できなくなった状態を示している。このような場合でも、正常に稼働している残りの３つのデータセンター１０ｂ、ｅ、ｇから３つの異なる部分データ５１０ａ、ｂ、ｃを集めることができ、重要データ５００を復元することができる場合があることを示している。

【００４１】

一方で、図４の例に示すように、５つ未満のデータセンター１０の障害等であっても、特定の部分データ５１０とそのコピーを保管するデータセンター１０に障害等が偏った場合などでは、重要データ５００の復元ができなくなる場合もある。図４の例では、４つのデータセンター１０ｃ、ｄ、ｇ、ｈにおいて障害等により部分データ５１０が取得できなくなった状態を示している。この場合、異なる部分データ５１０としては、部分データ５１０ａ、ｂの２つしか集めることができず、重要データ５００を復元することができない。

【００４２】

ここで、図４の例に示すような状態で、障害等となっているデータセンター１０のうちのいずれか１つが正常に稼働しているとした場合、当該データセンター１０から取得できる部分データ５１０は、部分データ５１０ｃもしくはｄのいずれかとなるため、取得可能な部分データ５１０ａ、ｂと合わせて、全体として異なる部分データ５１０を３つ集めることができることになり、重要データ５００を復元することが可能となる。ここから、３つのデータセンター１０の障害等であれば、いずれのデータセンター１０の障害等であっても必ず３つ以上の異なる部分データ５１０を集めることができ、重要データ５００を復元することが可能であることが分かる。

【００４３】

上述したように、例えば、重要データ５００から（３，４）閾値型の秘密分散により４つの部分データ５１０を生成し、これらを４つのデータセンター１０にそれぞれ分散保管した場合、そのうちの１つのデータセンター１０での障害等には耐えることができる。ここで、図２の例に示したように４つの部分データ５１０とそれらのコピーを、８つの異な

るデータセンター１０に二重化して分散保管した場合、データの保管に要するリソースの量としては２倍必要となる。一方で、耐えることができるデータセンター１０の障害等の数は、２倍の２つではなく、上述したように、最低でも３つ、最大で５つとなり、全体としてデータの可用性が２倍以上向上することになる。

【００４４】

上記の内容を一般化すると、重要データ５００から（ｋ，ｎ）閾値型の秘密分散によりｎ個の部分データ５１０を生成し、これらをｎ個の異なるデータセンター１０に分散保管した場合、そのうちの（ｎ－ｋ）個のデータセンター１０の障害等には耐えられるが、ｎ個の部分データ５１０およびそれらのコピーを、２ｎ個の異なるデータセンター１０に分散保管した場合、耐えることができるデータセンター１０の障害等の数は、２倍の２（ｎ－ｋ）個ではなく、最低でも（２（ｎ－ｋ）＋１）個、最大で（２ｎ－ｋ）個となる。ここで、１＜ｋ≦ｎの場合、２（ｎ－ｋ）＜（２（ｎ－ｋ）＋１）＜（２ｎ－ｋ）であることから、全体としてデータの可用性が２倍以上向上することになる。

【００４５】

＜システム構成＞

以下では、本実施の形態のデータ分散保管システム１のシステム構成について説明する。図１は、本発明の一実施の形態であるデータ分散保管システム１の構成例について概要を示した図である。データ分散保管システム１は、インターネット等のネットワーク４００に対して、複数のサーバ１００、マスタサーバ２００、およびクライアント端末３００が接続する構成を有する。なお、上述したように、各サーバ１００は、地理的にも組織的にも相互に関連のないデータセンター１０内においてそれぞれ運用管理されているものとする。また、サーバ１００（データセンター１０）の数は、重要データ５００から（ｋ，ｎ）閾値型の秘密分散によって生成されるｎ個の部分データ５１０に対して、２ｎ個以上が利用可能となるようにする。

【００４６】

サーバ１００は、サーバ機器によって構成されるコンピュータシステムであり、ファイルサーバもしくはストレージサーバ等として、ユーザ認証を経た後にクライアント端末３００等からのアクセスを受け付けてデータ（部分データ５１０）の保管サービスを提供する機能を有する。サーバ１００は、例えば、磁気ディスク等のストレージ機器からなるデータ保管部１１０およびソフトウェアプログラムにより実装される認証処理部１２０を有する。データ保管部１１０は、ＯＳ（Operating System）などの指示に基づいて、指定されたデータについての読み書きを行う。

【００４７】

認証処理部１２０は、サーバ１００へのアクセスに対しての認証処理を行う。認証処理部１２０は、認証処理を行う際に利用する情報として、ユーザ毎のアカウント情報からなるユーザ情報１３０を有する。ユーザ情報１３０は、例えば、データベースやファイルテーブル等によって構成され、例えば、登録されたユーザのユーザＩＤ毎に、ユーザ毎に異なる固有情報としてのユーザシーズ１３１、およびパスワードを所定の手順によりハッシュ化したハッシュ化パスワード１３２などのアカウント情報を有する。また、認証処理部１２０は、サーバ毎に異なる固有情報としてのサーバシーズ１４０を有する。

【００４８】

本実施の形態では、認証処理部１２０は、後述するように、クライアント端末３００との間でチャレンジ／レスポンス方式により認証処理を行う。すなわち、ユーザからの認証要求に対して、サーバシーズ１４０、ユーザシーズ１３１、およびチャレンジとしての乱数等を送信する。さらに、これらによってハッシュ化されたパスワード（ハッシュ値）をクライアント端末３００からレスポンスとして受信して、受信したハッシュ値と、ハッシュ化パスワード１３２を上記乱数によってハッシュ化したものとを比較して認証を行う。従って、認証処理部１２０は、乱数生成の機能やハッシュアルゴリズムを実装している。なお、これらの実装には公知の各種技術やアルゴリズムを利用することができる。サーバ１００とクライアント端末３００との間の通信経路のセキュリティが確保されるなどの場

合には、チャレンジ／レスポンス方式以外の他の方式を採用するなどしてもよい。

【００４９】

マスタサーバ２００は、サーバ機器やＰＣ等によって構成されるコンピュータシステムであり、各サーバ１００に保持するユーザシーズ１３１およびサーバシーズ１４０を生成して提供する。各サーバ１００を代表して認証を行ういわゆる認証サーバではないため、ユーザ認証の機能は有さない。マスタサーバ２００は、例えば、ソフトウェアプログラムにより実装されるシーズ生成部２１０を有する。シーズ生成部２１０は、管理者等からの指示もしくは各サーバ１００からの要求等に基づいてシーズを生成し、ユーザシーズ１３１もしくはサーバシーズ１４０として、対象のサーバ１００にネットワーク４００を介して提供する。

【００５０】

シーズの生成方法やシーズのフォーマット等については特に限定されないが、例えば、所定の長さのユニークな文字列やバイナリデータを生成してシーズとすることができる。なお、マスタサーバ２００は、他のサーバ１００とは独立したデータセンター１０に設置されていてもよいし、いずれかのサーバ１００と同一のデータセンター１０に、外部からアクセス可能な構成により設置されていてもよい。

【００５１】

クライアント端末３００は、重要データ５００から秘密分散技術を利用して部分データ５１０を複数生成し、さらに各部分データ５１０のコピーを生成して、これらをそれぞれ重複しないように各サーバ１００（各データセンター１０）に振り分けて送信し、データ保管部１１０に分散保管する機能を有する。クライアント端末３００は、例えば、ソフトウェアプログラムにより実装される分割処理部３１０、分散管理部３２０、復元処理部３３０、認証要求部３４０およびインタフェース部３５０の各部と、データベースもしくはファイルテーブル等からなる分散状況３２１および設定情報３０１の各テーブルを有する。

【００５２】

分割処理部３１０は、後述するインタフェース部３５０を介してユーザからセキュアな保管を指示された重要データ５００から、設定情報３０１の設定内容等に従って秘密分散により各サーバ１００に分散保管する複数の部分データ５１０を生成する。上述したように、秘密分散の手法は特に限定されず、公知の（ｋ，ｎ）閾値型の秘密分散の手法を用いることができる。設定情報３０１には、例えば、利用する秘密分散のアルゴリズムを特定する情報や、ｋ、ｎなどのパラメータを予め設定しておくことができる。

【００５３】

分散管理部３２０は、重要データ５００の分散保管の際に、分割処理部３１０によって秘密分散により生成された各部分データ５１０について、それぞれコピーを生成し、これらを設定情報３０１の設定内容に基づく所定の条件に従って各サーバ１００に送信して分散保管するとともに、各部分データ５１０がいずれのサーバ１００に保管されているかの対応に係る情報を分散状況３２１に記録して管理する。

【００５４】

各部分データ５１０をそれぞれどのサーバ１００に保管するかを決定する手法については種々のものが考えられる。図５は、部分データ５１０を保管するサーバ１００の選択の例について示した図である。図５の例では、各重要データ５００（“重要データα”、“重要データβ”、“重要データγ”、…）から（３，４）閾値型の秘密分散により生成した４つの部分データ５１０（“Ａ”、“Ｂ”、“Ｃ”、“Ｄ”）およびそれらのコピー（“ａ”、“ｂ”、“ｃ”、“ｄ”）に対して、１０個のサーバ１００（“サーバ＃１”～“サーバ＃１０”）から保管先となるサーバ１００を８つ選択して割り当てた場合を示している。

【００５５】

例えば、各サーバ１００（“サーバ＃１”～“サーバ＃１０”）をランダムあるいはスペック等に基づく優先順位等に従って順序付けしておき、そこからその時点で障害等によ

り稼動していないサーバ１００（図５の例では、“重要データγ”を保管する際の“サーバ＃６”）を除外した上で、リストの順序に従って２ｎ個のサーバ１００を順に選択するようにしてもよい。このとき、毎回リストの先頭（例えば“サーバ＃１”）から２ｎ個のサーバ１００を選択するようにしてもよいし、図５の例に示すように、選択する際の始点を保管する重要データ５００毎にずらして、選択するサーバ１００をローテーションするようにしてもよい。

【００５６】

選択するサーバ１００をローテーションすることで、複数の重要データ５００について、部分データ５１０の分散保管のされ方がそれぞれ異なるようにすることができる。これにより、例えば、複数のサーバ１００（図５の例では、網掛けされた“サーバ＃１”、“サーバ＃２”、“サーバ＃５”、“サーバ＃６”の４つ）で障害等により部分データ５１０の取得が不能となった場合に、復元できなくなる重要データ５００の範囲を一部に抑え（図５の例では“重要データα”のみ）、全ての重要データ５００が復元不能となるような事態を防止することができる。

【００５７】

選択した２ｎ個のサーバ１００に対して部分データ５１０を割り当てる手法についても種々のものが考えられる。例えば、図５の例に示すように、２ｎ個のサーバ１００のリストに対して、ｎ個の部分データ５１０、ｎ個のコピーの順で順次割り当てるようにしてもよいし、各部分データ５１０をランダムに割り当てるようにしてもよい。また、ある部分データ５１０とそのコピーが相互に地理的に近いサーバ１００（データセンター１０）に保管されないように、例えば、２ｎ個のサーバ１００のリストを地理的距離に基づいて予め２つのグループに分類してから、それぞれのグループに属するサーバ１００に、部分データ５１０とそのコピーをそれぞれ分離して割り当てる等の考慮を行ってもよい。

【００５８】

設定情報３０１には、例えば、分散保管先となる各サーバ１００に対するアクセス情報（ＩＰアドレスやホスト名等）、複数のサーバ１００の中から２ｎ個のサーバ１００を選択し、部分データ５１０とそのコピーを割り当てるための基準や条件（例えばサーバ１００の優先順位や順序付けされたリスト、ローテーションの際の方法等）などを予め設定しておくことができる。

【００５９】

また、分散管理部３２０は、後述する復元処理部３３０による重要データ５００の復元の際に、復元処理部３３０からの要求に基づいて、分散状況３２１の内容、および設定情報３０１の設定内容に基づく所定の条件に従って、各サーバ１００から、重要データ５００を復元するための異なるｍ個の部分データ５１０（もしくはそのコピー）を収集して復元処理部３３０に受け渡す。

【００６０】

なお、収集する部分データ５１０の個数ｍの値は、重要データ５００を復元するために必要な閾値ｋ以上である必要があり、また、ｎ個全ての部分データ５１０を収集するものとしてもよい（ｋ≦ｍ≦ｎ）。設定情報３０１には、例えば、ｍの値や、ｍ＜ｎである場合に、対象となるｍ個のサーバ１００を選択するための基準や条件、障害等により対象のサーバ１００から部分データ５１０を取得できなかった場合の代替となるサーバ１００の決定方法（例えば、取得できなかった部分データ５１０に対するコピーを取得するのか、他の部分データ５１０を取得するのか等）などを予め設定しておくことができる。

【００６１】

なお、サーバ１００の障害等により、例えば、部分データ５１０の分散保管時にｎ個の部分データ５１０のうちいずれかとそのコピーの双方とも各サーバ１００に保管できなかった場合や、部分データ５１０の収集時に異なるｋ個以上を収集できなかったなどの場合は、ユーザに対してエラーを応答するようにしてもよい。また、各サーバ１００との間で部分データ５１０の送受信を行う際に、クライアント端末３００および各サーバ１００がそれぞれ部分データ５１０に対して所定の暗号化を施した上で送受信することで、情報漏

洩のリスクをさらに低減させるようにしてもよい。

【００６２】

復元処理部３３０は、インタフェース部３５０を介してユーザから参照や編集等の利用を指示された重要データ５００について、これを復元するために必要な数以上の異なる部分データ５１０を分散管理部３２０に要求して取得し、取得した部分データ５１０から秘密分散の手法により重要データ５００を復元する。

【００６３】

認証要求部３４０は、分散管理部３２０が各サーバ１００に対して部分データ５１０を分散保管する際、および各サーバ１００から部分データ５１０を収集する際の、各サーバ１００に対する認証の要求を行う。例えば、ログイン画面を介してユーザからユーザＩＤおよびパスワードの入力を受け付け、後述するように、チャレンジ／レスポンス方式等により、各サーバ１００の認証処理部１２０との間で順次もしくは並行的にそれぞれ個別に認証処理を行うことで、シングルサインオンの機能を実現する。

【００６４】

ここでは、後述するように、認証要求の送信に対してサーバ１００の認証処理部１２０から送信されたサーバシーズ１４０、ユーザシーズ１３１、および乱数に基づいて、ユーザから指定されたパスワードを所定の手順によりハッシュ化し、これをサーバ１００の認証処理部１２０に送信することで認証処理を行う。従って、認証要求部３４０は、サーバ１００の認証処理部１２０が実装しているものと同一のハッシュアルゴリズムを実装している。

【００６５】

インタフェース部３５０は、クライアント端末３００における画面表示等のユーザインタフェースやデータの送受信などの入出力機能を有する。ユーザは、例えば、一般的なＯＳが有するファイル管理用の画面等を利用して、データ分散保管システム１の機能を利用することができる。

【００６６】

例えば、ファイル管理用の画面において重要データを特定のフォルダ等にドラッグ＆ドロップなどの簡易な操作により移動する。これをトリガとして、分割処理部３１０および分散管理部３２０によって、自動的に当該重要データ５００から（ｋ，ｎ）閾値型の秘密分散によりｎ個の部分データ５１０を生成し、各部分データ５１０をユーザに意識させずに各サーバ１００に分散保管することができる。なお、上述したように、このとき重要データ５００はクライアント端末３００から削除するが、ファイル管理用の画面上では、ユーザに意識させないよう、例えば、重要データ５００に対応するダミーファイル等を作成して残しておく。

【００６７】

また、例えば、ユーザは、ファイル管理用の画面において特定のフォルダにて管理されている重要データ５００のダミーファイル等に対して操作を行うことで、重要データ５００に対する参照や編集等の操作を行うことができる。すなわち、ダミーファイル等に対する操作をトリガとして、分散管理部３２０および復元処理部３３０によって、ダミーファイル等に対応する重要データ５００について、自動的に各サーバ１００から異なるｍ個（ｋ≦ｍ≦ｎ）の部分データ５１０を収集し、重要データ５００を復元してユーザに利用可能とすることができる。

【００６８】

＜認証処理＞

以下では、本実施の形態のデータ分散保管システム１における認証処理の内容について説明する。本実施の形態のデータ分散保管システム１では、上述したように、複数のサーバ１００に対して部分データ５１０を分散保管する際、および複数のサーバ１００から部分データ５１０を収集する際に、ユーザによる各サーバ１００に対する個別の認証処理に伴う煩雑さを回避するため、シングルサインオンの仕組みを有する。

【００６９】

シングルサインオンの環境を実現する手法としては、例えば、各サーバ１００がＳＡＭＬ（Security Assertion Markup Language）プロトコル等を用いてサーバ１００間で通信を行って、認証サーバ等の特定のサーバで行った認証結果の情報を自動的に引き継ぐことで、各サーバ１００でのユーザによる再度の認証手続きを不要とする手法などがある。

【００７０】

しかしながら、このような手法によるシングルサインオンの環境は、例えば、イントラネット上の社内システムなど、サーバ１００間で認証情報の引き継ぎ・受け入れを許容する信頼関係が成立していることが前提となる。従って、本実施の形態のように、各データセンター１０が地理的にも組織的にも関連のないものである場合は、セキュリティ上の関係等からこのような信頼関係が成立しない場合もある。

【００７１】

また、このような環境で上述したようなシングルサインオンの手法を用いると、例えば、あるサーバ１００において、ユーザの認証処理のために認証サーバ等から取得した認証情報を、悪意を持った内部の者が利用して他のサーバ１００に対して不正にアクセスを行い、当該他のサーバ１００に保管されている部分データ５１０を取得してしまうということも考えられる。従って、本実施の形態のようなデータ分散保管システム１の環境では、各サーバ１００（データセンター１０）間での部分データ５１０の不正取得を防止するためのセキュリティについても考慮する必要がある。

【００７２】

本実施の形態では、例えば代表となる認証サーバ等での認証結果をＳＡＭＬプロトコル等によって各サーバ１００間で引き継ぐような認証手法ではなく、各データセンター１０間で異なる固有情報（鍵）を用いて個別に認証処理を行うことで、各データセンター１０へのアクセスを独立して安全に行える仕組みを有し、各データセンター１０間でのセキュリティを確保する。

【００７３】

認証処理を行うに当たっての初期状態として、各サーバ１００では、予め、マスタサーバ２００のシーズ生成部２１０によって生成されたシーズをそれぞれサーバシーズ１４０として保持しているものとする。さらに、各ユーザによって、ユーザＩＤ、パスワード等を含むアカウント情報の初期登録が事前に行われているものとする。このとき、アカウント情報として、ユーザＩＤ毎にそれぞれマスタサーバ２００のシーズ生成部２１０によって生成されたシーズをユーザシーズ１３１として保持しておく。さらに、パスワードについては、当該ユーザシーズ１３１およびサーバシーズ１４０をシード値として、所定のハッシュアルゴリズムによりハッシュ化したハッシュ化パスワード１３２として保持しておく。

【００７４】

パスワードを直接保持しないことで、パスワードの漏洩を防止することができる。また、ユーザ毎にユニークなユーザシーズ１３１をシード値としてハッシュ化を行うことで、例えば、複数のユーザによって偶然同一のパスワードが指定された場合でも、ユーザ毎にハッシュ値が異なるようにすることができる。

【００７５】

図６は、本実施の形態における認証処理の流れの例について概要を示した図である。まず、ユーザはクライアント端末３００の認証要求部３４０を介して、認証（ログイン）の要求を行う。このとき、例えば、ユーザＩＤおよびパスワードの情報をログイン画面等を介して指定する。認証要求部３４０は、指定されたユーザＩＤを含む認証の要求をサーバ１００へ送信する（Ｓ０１）。

【００７６】

ユーザＩＤを受信したサーバ１００の認証処理部１２０は、チャレンジ／レスポンス方式におけるチャレンジとしての乱数を生成し、さらにシーズを取得して、これらをクライアント端末３００に送信する（Ｓ０２）。ここでは、乱数に加えて、サーバシーズ１４０と、ユーザ情報１３０に保持されたユーザＩＤに対応するユーザシーズ１３１を取得する

。

【００７７】

サーバシーズ１４０とユーザシーズ１３１、および乱数を受信したクライアント端末３００の認証要求部３４０では、ステップＳ０１において指定されたパスワードを所定のハッシュアルゴリズムによりハッシュ化する（Ｓ０３）。さらに、ステップＳ０３で得られたハッシュ値を、ユーザシーズ１３１をシード値としてハッシュ化する（Ｓ０４）。さらに、ステップＳ０４で得られたハッシュ値を、サーバシーズ１４０をシード値としてハッシュ化する（Ｓ０５）。さらに、ステップＳ０５で得られたハッシュ値を、乱数をシード値としてハッシュ化することでワンタイム化し、得られたハッシュ値をサーバ１００へ送信する（Ｓ０６）。

【００７８】

なお、上記のステップＳ０３～Ｓ０５の一連のハッシュ化処理手順は、一例であり、同等の結果が得られる他の手順とすることも当然可能であるが、事前のユーザ登録の際にパスワードをハッシュ化してハッシュ化パスワード１３２を取得する際のハッシュ化処理と同一の手順である必要がある。また、例えば、ステップＳ０２において、サーバ１００からパスワードの有効期限が経過しているためパスワードを更新する旨の指示を受信した場合など、必要に応じて、ステップＳ０３を実行する前にパスワード（およびハッシュ化パスワード１３２）の更新を行えるようにしてもよい。

【００７９】

ハッシュ値を受信したサーバ１００の認証処理部１２０は、ユーザ情報１３０から対象のユーザＩＤに対応するハッシュ化パスワード１３２を取得し（Ｓ０７）、取得したハッシュ化パスワード１３２を、ステップＳ０２で生成した乱数をシード値としてハッシュ化する（Ｓ０８）。その後、得られたハッシュ値と、ステップＳ０７でクライアント端末３００から受信したハッシュ値とを比較することで認証処理を行い、認証結果をクライアント端末３００に送信する（Ｓ０９）。すなわち、比較の結果両者が一致すれば認証は成立し、不一致であれば認証は不成立となる。なお、このとき例えば、クライアント端末３００からの要求電文からＩＰアドレス等の発信元の所在に係る情報を取得し、当該情報が所定の範囲内にあるか否か等の他の条件を認証の成否の判断に加えてもよい。

【００８０】

クライアント端末３００の認証要求部３４０は、認証結果を受領し（Ｓ１０）、その後、必要に応じて他のサーバ１００に対しても順次上記の一連の処理を自動的に行い、各サーバ１００に対する認証処理を行う。各サーバ１００での認証処理は独立していることから、必要な複数のサーバ１００に対して上記の一連の処理を同時並行的に行うことも可能である。なお、必要なサーバ１００の情報については、例えば、クライアント端末３００の設定情報３０１等に予め設定しておいてもよいし、分散管理部３２０が、部分データ５１０の分散保管時や収集時に選択したサーバ１００を対象としてもよい。

【００８１】

以上の処理により、ユーザは、ユーザＩＤおよびパスワードの指定を１回行うだけで、必要な各サーバ１００に対して認証処理を行うことができる。

【００８２】

上述したような手法をとることにより、例えば、あるサーバ１００やデータセンター１０の管理者等が、対象のユーザのユーザシーズ１３１やハッシュ化パスワード１３２などのアカウント情報を自身のユーザ情報１３０から取得したとしても、これらの情報を利用して他のサーバ１００（データセンター１０）に対してなりすましによる認証を行うことはできず、サーバ１００間でのセキュリティは確保される。

【００８３】

これは、あるサーバ１００でのユーザのハッシュ化パスワード１３２の値は、自身のサーバシーズ１４０によってハッシュ化されたものであり、他のサーバ１００における当該ユーザのハッシュ化パスワード１３２は、当該他のサーバ１００のサーバシーズ１４０によってハッシュ化されたものであるため値が異なるからである。従って、両者を同じ乱数

をシード値としてハッシュ化しても同一のハッシュ値とはならず、図６のステップＳ０９において認証は不成立となる。また、当該他のサーバ１００のサーバシーズ１４０を何らかの手段で取得してきたとしても、対象のユーザのパスワードを知らない限り、当該他のサーバ１００におけるハッシュ化パスワード１３２と同じ値のハッシュ値を生成することはできない。

【００８４】

以上に説明したように、本発明の一実施の形態であるデータ分散保管システム１によれば、重要データ５００から秘密分散技術により部分データ５１０を生成して各データセンター１０に分散保管することで、クライアント端末３００の盗難や紛失等による重要データ５００の漏洩を防止することができる。また、各データセンター１０は重要データ５００につき部分データ５１０を１つしか有していないため、データセンター１０に対して第三者が侵入して不正に部分データ５１０を取得したり、データセンター１０の管理者等の内部の者が部分データ５１０を取得したりした場合でも、部分データ５１０を１つしか得ることができない。当該部分データ５１０だけでは重要データ５００を復元・推測することはできないため、重要データ５００の内容が漏洩することはない。

【００８５】

また、各部分データ５１０を複数のデータセンター１０に送信して分散保管する際に、各部分データ５１０のコピーをそれぞれ別のデータセンター１０に保管して二重化する。これにより、使用する秘密分散のライブラリの機能や仕様に依存せず、必要となるリソースの増加量に比して、データの可用性を大きく向上させることができる。

【００８６】

また、サーバ１００毎に異なる固有情報（サーバシーズ１４０）を用いて認証を行うことで、データセンター１０の管理者等の内部の者が、悪意を持って他のデータセンター１０にアクセスすることも困難であることから、各データセンター１０間での部分データ５１０の不正取得を防止するためのセキュリティを確保することが可能となる。

【００８７】

また、ユーザによるクライアント端末３００からの一度の認証処理によって複数のサーバ１００に対するシングルサインオンを実現することができ、また、各サーバ１００での認証を同時並行的に行うことが可能である。従って、重要データ５００から生成された部分データ５１０の分散保管、および重要データ５００を復元するために必要な数以上の部分データ５１０の収集において、認証に要する時間を削減してレスポンスの低下を抑止することが可能となる。

【００８８】

以上、本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【産業上の利用可能性】

【００８９】

本発明は、重要データから秘密分散技術により複数の非重要データを生成して複数の拠点に分散保管するデータ分散保管システムに利用可能である。

【符号の説明】

【００９０】

１…データ分散保管システム、

１０、１０ａ～ｈ…データセンター、

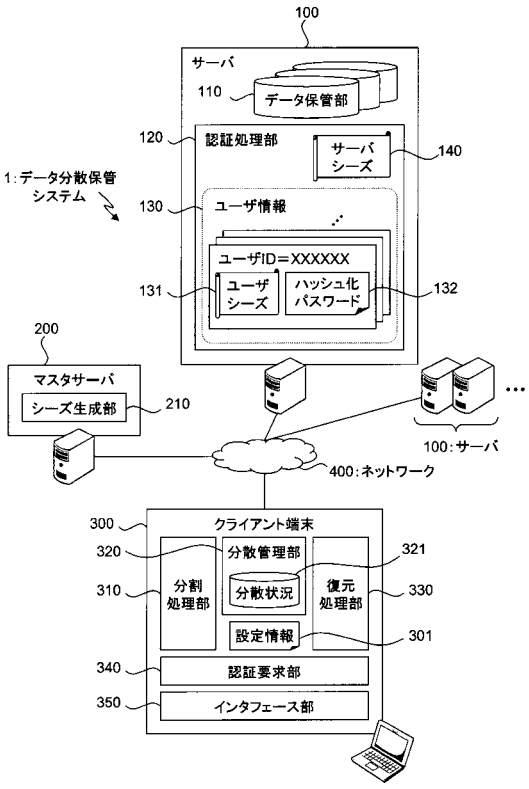
１００…サーバ、１１０、１１０ａ～ｈ…データ保管部、１２０…認証処理部、１３０…ユーザ情報、１３１…ユーザシーズ、１３２…ハッシュ化パスワード、１４０…サーバシーズ、

２００…マスタサーバ、２１０…シーズ生成部、

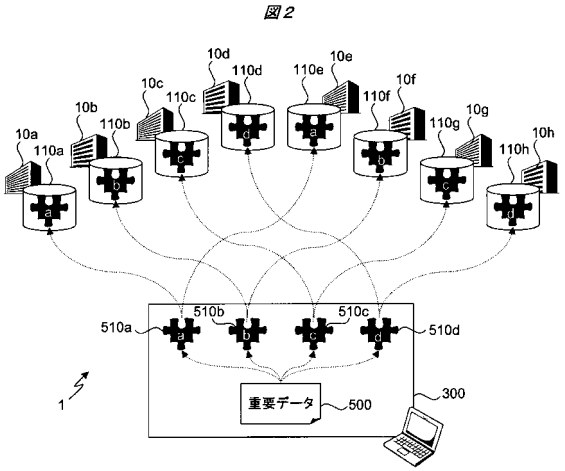
３００…クライアント端末、３０１…設定情報、３１０…分割処理部、３２０…分散管理部、３２１…分散状況、３３０…復元処理部、３４０…認証要求部、３５０…インタフ

ェース部、
４００…ネットワーク、
５００…重要データ、５１０ａ～ｄ…部分データ。
【要約】
【課題】重要データから秘密分散技術により生成された複数の部分データを複数のデータセンターに分散保管するにあたり、秘密分散を実装するライブラリ等に依存せずにデータの可用性を向上させるデータ分散保管システムを提供する。
【解決手段】各サーバ１００はクライアント端末３００から受信した部分データを保管するデータ保管部１１０を有し、クライアント端末３００は、重要データから秘密分散技術によりｋ個以上集めなければ重要データを復元できないｎ個（ｋ≦ｎ）の部分データを生成する分割処理部３１０と、ｎ個の部分データおよびｎ個のコピーを２ｎ個のサーバ１００に保管し、重要データを復元するためのｍ個（ｋ≦ｍ≦ｎ）の異なる部分データもしくはコピーをｍ個のサーバ１００から収集する分散管理部３２０と、ｍ個の部分データもしくはコピーから秘密分散技術により重要データを復元する復元処理部３３０とを有する。
【選択図】図１

【図１】

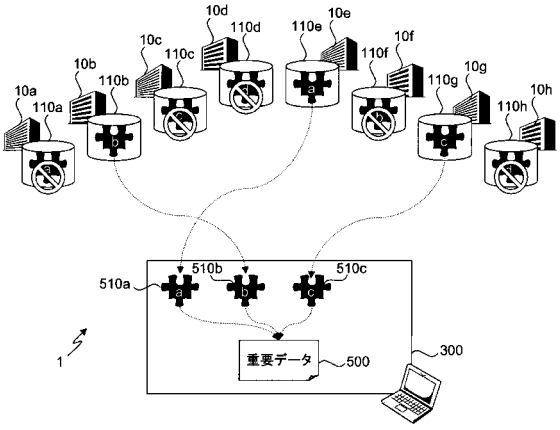


【図２】



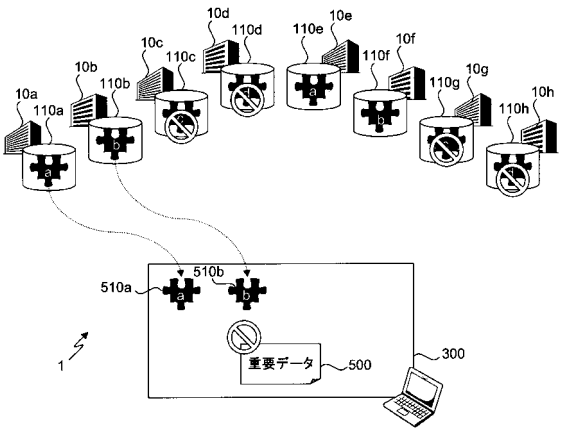
【図３】

図3



【図４】

図4



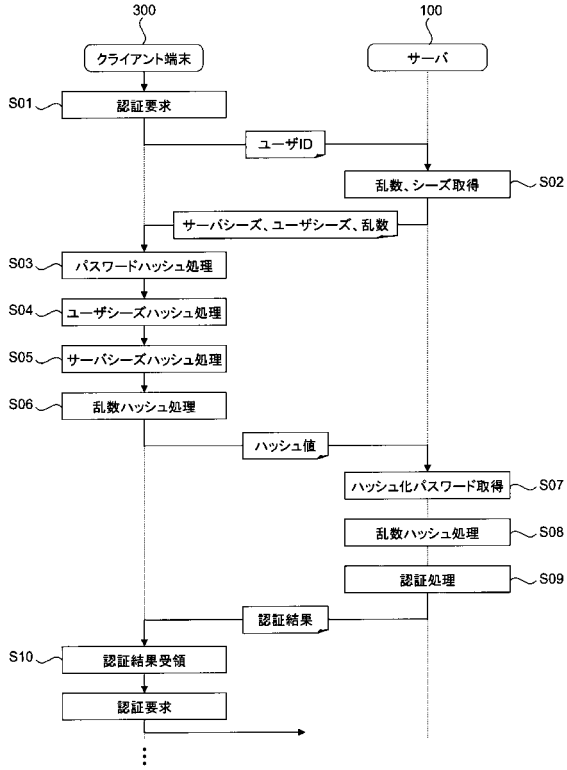
【図５】

図5

	サーバ#1	サーバ#2	サーバ#3	サーバ#4	サーバ#5	サーバ#6	サーバ#7	サーバ#8	サーバ#9	サーバ#10	
重要データα	A	B	C	D	a	b	c	d			→×
重要データβ		A	B	C	D	a	b	c	d		→○
重要データγ	d		A	B	C	×	D	a	b	c	→○
…	…	…	…	…	…	…	…	…	…	…	

【図６】

図6



フロントページの続き

(72)発明者　最首　壮一
東京都港区東新橋一丁目５番２号　汐留シティセンター　エヌ・アール・アイ・セキュアテクノロジーズ株式会社内

審査官　後藤　彰

(56)参考文献　特開２００７－１０２６７２（ＪＰ，Ａ）
特開２００５－２１５７３５（ＪＰ，Ａ）
特開２００９－０１０５３１（ＪＰ，Ａ）
特開２００５－２０９１１８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２４