(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6427661号
(P6427661)
(45)発行日　平成30年11月21日(2018.11.21)　(24)登録日　平成30年11月2日(2018.11.2)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62 309
G06F 21/62 345

請求項の数 27　(全 21 頁)

(21)出願番号　特願2017-508674 (P2017-508674)
(86)(22)出願日　平成27年8月12日 (2015.8.12)
(65)公表番号　特表2017-527900 (P2017-527900A)
(43)公表日　平成29年9月21日 (2017.9.21)
(86)国際出願番号　PCT/KR2015/008458
(87)国際公開番号　WO2016/028027
(87)国際公開日　平成28年2月25日 (2016.2.25)
審査請求日　平成29年2月22日 (2017.2.22)
(31)優先権主張番号　10-2014-0107267
(32)優先日　平成26年8月18日 (2014.8.18)
(33)優先権主張国　韓国 (KR)

(73)特許権者　514180694
ナム、ギ　ウォン
ＮＡＭ，Ｋｉ－Ｗｏｎ
大韓民国、１３５－８７７、ソウル、カンナム－グ、テヘラン－ロ、４２３（サムソン－ドン、ヒョンデ　タワー）＃１３０２
＃１３０２（Ｈｙｕｎｄａｉ　Ｔｏｗｅｒ，Ｓａｍｓｕｎｇ－ｄｏｎｇ）４２３，Ｔｅｈｅｒａｎ－ｒｏ，Ｇａｎｇｎａｍ－ｇｕ　Ｓｅｏｕｌ　１３５－８７７，Ｒｅｐｕｂｌｉｃ　ｏｆ　Ｋｏｒｅａ
(74)代理人　100130111
弁理士　新保　斉

最終頁に続く

(54)【発明の名称】個人データ管理システム及びその方法

(57)【特許請求の範囲】
【請求項１】
ａ）ユーザ端末２にインストールされた個人データ管理アプリケーション６が駆動信号を受信する段階と；
ｂ）データ分散選択信号が印加されたか否かを前記個人データ管理アプリケーション６が判断する段階と；
ｃ）特定データが選択されたか否かを前記個人データ管理アプリケーション６が判断する段階と；
ｄ）前記個人データ管理アプリケーション６がデータ伝送先の情報をデータ管理サーバ１０に要求する段階と；
ｅ）前記データ管理サーバ１０がデータ伝送先の情報を前記個人データ管理アプリケーション６に提供する段階と；
ｆ）前記個人データ管理アプリケーション６がデータを所定数のデータに分割処理する段階と；
ｇ）各分割データをデータ伝送先の端末側とランダムにマッチングさせて伝送する段階と；を含む
ことを特徴とする個人データの管理方法。
【請求項２】
前記ｅ）段階は、前記データ管理サーバ１０が格納先となる端末識別情報プール（Ｐｏｏｌ）から所定数の識別情報をランダムに抽出する段階を更に含む

請求項１に記載の個人データの管理方法。
【請求項３】
前記ｆ）段階は、前記個人データ管理アプリケーション６が前記データ管理サーバ１０から提供されたデータ伝送先の端末のうち一部をランダムに抽出することによって、最終伝送先の端末を決定する段階を更に含む
請求項１に記載個人データの管理方法。
【請求項４】
前記ｇ）段階は、前記個人データ管理アプリケーション６が分割されたバックアップデータを別のデータバックアップ先の端末に伝送する段階を更に含む
請求項１に記載の個人データの管理方法。
【請求項５】
前記ｇ）段階の後に、
ｈ）前記個人データ管理アプリケーション６がデータ復旧モードが選択されたか否かを判断する段階と；
ｉ）特定データ復旧信号が受信されると、前記個人データ管理アプリケーション６がデータの分割データを分散格納する格納先端末情報を抽出する段階と；
ｊ）前記個人データ管理アプリケーション６がデータの格納先端末にデータ伝送要求の処理を行って、データを受信する段階と；
ｋ）データの受信が完了すると、前記個人データ管理アプリケーション６がデータを復旧する段階を更に含む
請求項１に記載の個人データの管理方法。
【請求項６】
前記ｋ）段階は、一部の端末から、前記個人データ管理アプリケーション６がデータの格納先端末にデータ伝送要求の処理を行った時点から一定時間の経過時までデータが受信されないと、前記個人データ管理アプリケーション６がデータのバックアップ格納先の端末情報を抽出する段階と；
前記個人データ管理アプリケーション６がバックアップ格納先の端末側にデータ伝送要求の処理を行う段階を更に含む
請求項５に記載の個人データの管理方法。
【請求項７】
前記ｇ）段階の後に、前記個人データ管理アプリケーション６が前記データ管理サーバ１０にデータ伝送先の端末情報を伝送する段階を更に含む
請求項１に記載の個人データの管理方法。
【請求項８】
前記ｈ）段階とｉ）段階との間には、
ｌ）前記個人データ管理アプリケーション６が復旧するデータ情報を前記データ管理サーバ１０に伝送し、データの認証ユーザ情報を要求する段階と；
ｍ）前記データ管理サーバ１０がデータの認証ユーザ情報を個人データ管理アプリケーション６に伝送する段階と；
ｎ）前記個人データ管理アプリケーション６が認証ユーザ端末２に個人認証情報の入力を要求する段階と；
ｏ）認証ユーザ端末２で個人認証成功時に認証ユーザのユーザ端末２は前記個人データ管理アプリケーション６に認証確認信号を伝送する段階を更に含む
請求項５に記載の個人データの管理方法。
【請求項９】
前記ｍ）段階は、前記データ管理サーバ１０がショートメッセージや電子メールを通じて認証ユーザ情報を個人データ管理アプリケーション６に伝送する段階である
請求項８に記載の個人データの管理方法。
【請求項１０】
前記ｏ）段階は、認証失敗信号が前記認証ユーザ端末２から受信されると、前記個人デ

ータ管理アプリケーション６は前記データ管理サーバ１０に認証失敗情報を伝送する段階と；

前記個人データ管理アプリケーション６が認証ユーザ端末２に個人認証情報の入力を要求した時点から所定時間の経過時まで認証信号が受信されないと、個人データ管理アプリケーション６は前記データ管理サーバ１０に新規な認証ユーザ情報を要求する信号を伝送する段階と；

前記データ管理サーバ１０が個人データ管理アプリケーション６に新規な認証ユーザ情報を伝送する段階を更に含む

請求項８に記載の個人データの管理方法。

【請求項１１】

前記ｋ）段階は、前記個人データ管理アプリケーション６がデータの格納先端末にデータ伝送要求の処理を行った時点から所定時間の経過時まで特定の分割データが受信されたか否かを判断する段階と；

特定の分割データが受信されない時、バックアップデータを格納するユーザ端末情報を抽出する段階と；

前記個人データ管理アプリケーション６がバックアップデータを格納するユーザ端末２側にデータ伝送を要求する段階を更に含む

請求項５に記載の個人データの管理方法。

【請求項１２】

データを分割して伝送する伝送ユーザ端末２－１と、分割格納したデータを復旧しようとする受信ユーザ端末２－３が互いに異なる場合、前記伝送ユーザ端末２－１は前記受信ユーザ端末２－３側に前記伝送ユーザ端末２－１により分割されて格納されるデータと、受信認証情報と、残りの分割データの格納端末情報を伝送する段階を更に含む

請求項１に記載の個人データの管理方法。

【請求項１３】

ユーザ認証により駆動され、ユーザが選択した特定データを複数のデータに自動分離して、データ管理サーバ１０から伝送された特定識別番号の複数の第２ユーザ端末２－２に分散して伝送し、ユーザの復旧指令に応じて分散データをまとめて復旧させる個人データ管理アプリケーション６がインストールされた第１ユーザ端末２－１と；

前記個人データ管理アプリケーション６がインストールされた第１ユーザ端末２－１の識別情報を格納し、前記第１ユーザ端末２－１からデータの分散信号を受けて、データの分散格納先となる特定のユーザ端末識別情報を抽出して前記第２ユーザ端末２－２に伝送処理するデータ管理サーバー１０と；を含む

ことを特徴とする個人データ管理システム。

【請求項１４】

前記データ管理サーバ１０は、特定のユーザ端末識別情報を抽出する際、格納先となる端末識別情報プール（Ｐｏｏｌ）から所定数の識別情報をランダムに抽出するように構成される

請求項１３に記載の個人データ管理システム。

【請求項１５】

前記個人データ管理アプリケーション６は、前記データ管理サーバ１０から提供されたユーザ端末識別情報のうち所定数の識別情報をランダムに抽出するように構成される

請求項１３に記載の個人データ管理システム。

【請求項１６】

データを分散して伝送する前記第１ユーザ端末２－１と、データを分散して伝送する前記第２ユーザ端末２－２、前記データ管理サーバ１０との間に伝送されるデータは暗号化されたデータである

請求項１３に記載の個人データ管理システム。

【請求項１７】

前記個人データ管理アプリケーション６は複数に分割されたデータのうちいずれかのデ

ータを第１ユーザ端末２－１に格納し、それ以外のデータは特定識別番号の複数の第２ユーザ端末２－２に分散して格納するように構成される
請求項１３に記載の個人データ管理システム。
【請求項１８】
前記個人データ管理アプリケーション６は、その内部に、データを分散格納する複数の第２ユーザ端末２－２及びデータ管理サーバ１０と通信する通信モジュール２０と、
個人識別情報の認証を通じてユーザを認証するユーザ認証部２２と、
前記データ管理サーバ１０にデータを分散格納する格納先情報を自動で要求する格納先情報要求部２４と；
ユーザが選択した特定データを分割処理するデータ分割処理部２８と、
通信データの暗号化及び復号化を行う暗号／復号処理部３２と；
分割処理したデータのうち一部のデータを格納し、各分割処理したデータが格納されている格納先情報を格納するデータ格納部３４と、
前記データ管理サーバ１０と通信してデータ格納先情報の提供を受け、特定データを分割して一部のデータは格納し、それ以外のデータは複数のデータ格納先端末に伝送して分散格納するように処理し、データの復旧時に格納先端末側に特定データの伝送要求信号を伝送して復旧を行う制御部３６と、を含む
請求項１３に記載の個人データ管理システム。
【請求項１９】
前記個人データ管理アプリケーション６は、その内部に、前記データ管理サーバ１０から受信した格納先情報のうち一部をランダムに抽出する格納先ランダム抽出部２６を更に含む
請求項１８に記載の個人データ管理システム。
【請求項２０】
前記個人データ管理アプリケーション６は、その内部に、分割されたデータとデータの格納先とがランダムにマッチングされるように処理する格納先ランダムマッチング部３０を更に含む
請求項１８に記載の個人データ管理システム。
【請求項２１】
前記個人データ管理アプリケーション６は、複数のデータ伝送先の端末に分割データを伝送し、同じ分割データをバックアップ先の端末側に伝送してバックアップ格納するように処理し、データの復旧時に一定時間内に特定の分割データの復旧が行われないと、バックアップデータを用いた復旧処理を行うように構成される
請求項１３に記載の個人データ管理システム。
【請求項２２】
前記データ管理サーバ１０は、特定データの復旧時に認証が必要な単一の認証ユーザ情報をデータ分散格納時に登録し、前記個人データ管理アプリケーション６のデータ復旧要求時に、認証ユーザ情報を個人データ管理アプリケーション６に提供するように構成される
請求項１３に記載の個人データ管理システム。
【請求項２３】
前記個人データ管理アプリケーション６は前記データ管理サーバ１０から認証ユーザ情報が提供されると、認証ユーザのユーザ端末２側に個人認証情報の入力を要求するように構成され、個人認証成功時に認証ユーザの第３ユーザ端末２－３は前記個人データ管理アプリケーション６に認証確認信号を伝送するように構成される
請求項２２に記載の個人データ管理システム。
【請求項２４】
前記データ管理サーバ１０が前記個人データ管理アプリケーション６に伝送する認証ユーザ情報は、テキストメッセージや電子メールを通じて伝送するように構成される
請求項２２に記載の個人データ管理システム。

【請求項２５】
前記個人データ管理アプリケーション６は、前記個人データ管理アプリケーション６が認証ユーザのユーザ端末２側に個人認証情報の入力を要求した時点から所定時間の経過時まで認証ユーザの認証確認情報が受信されないと、前記データ管理サーバ１０に新規な認証ユーザ情報を要求するように構成される
請求項２３に記載の個人データ管理システム。
【請求項２６】
元データを分割する前記第１ユーザ端末２－１と、元データを復旧する第３ユーザ端末２－３が互いに異なって構成される場合、前記第１ユーザ端末２－１は前記第３ユーザ端末２－３に前記第１ユーザ端末２－１により分割されて格納されるデータと、受信認証情報と、残りの分割データの格納端末情報を伝送するように構成される
請求項１３に記載の個人データ管理システム。
【請求項２７】
分散データを格納する前記複数の第２ユーザ端末２－２はサーバ、ＰＣ、及び無線端末のうちいずれか一つである
請求項１３に記載の個人データ管理システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は個人データ管理システム及びその方法に関するものであって、より詳細には、ユーザの個人データをユーザ端末や特定サーバーに格納せずにランダムに分散格納して管理し、必要に応じて複数の認証手続きを経てユーザ端末で個人データを復旧することによって、ハッキングを受ける可能性が大幅に低減すると共に、ユーザ端末の紛失時にもデータの流出を防止できる個人データ管理システム及びその方法に関するものである。
【背景技術】
【０００２】
最近、データ通信技術が急速に発展するにつれて、個人携帯端末機を通じてオンラインで送金の支払いなどの各種金融処理を行う。金融処理のためには個人を識別することができる識別情報が必要であり、その識別情報を含む個人情報は金融サーバーに格納されている。
従って、１つの金融サーバーには数百万件の大量の個人情報が格納されているので、金融サーバはハッカーが狙えるターゲットとなる。実際に多くの金融サーバーがハッキングを受けて、複数の個人情報が不法使用のために流通されている。
金融サーバーがハッカーの標的になる最大の理由は、活用可能な個人情報を非常に多く含んでいるためである。即ち、時間を有して努力してハッキングに成功した場合は、活用できる大量の個人情報が得られるので、頻繁にハッカーの標的になる。
一方、最近の携帯情報端末はデジタルカメラと無線インターネットが可能であるので、様々な私生活を撮像したデータを格納しているが、非常に頻繁に個人のプライバシーデータがインターネット上に流出して大変な苦労をする。特に、芸能人などのスターの場合は、個人のプライバシーデータが流出すると、全国民に及ぼすその波及効果が非常に大きいと言える。
【０００３】
これを防ぐための様々なセキュリティ技術が開発されているが、現実的にサーバーに格納されたデータをハッキングすることは不可能ではなく、個人携帯端末機に格納されたデータもハッキングして流出させる恐れがあるなどの問題がある。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
本発明は前述した従来技術の事情に鑑みてなされたものであって、ユーザの個人データ

をユーザ端末や特定サーバーに格納せずにランダムに分散格納して管理し、必要に応じて複数の認証手続きを経てユーザ端末で個人データを復旧することによって、ハッキングを受ける可能性が大幅に低減すると共に、ユーザ端末の紛失時にもデータの流出を防止できる個人データ管理システム及びその方法を提供することにその目的がある。

【課題を解決するための手段】

【０００５】

前述した目的を達成するための本発明に係る個人データの管理方法は、ａ）ユーザ端末２にインストールされた個人データ管理アプリケーション６が駆動信号を受信する段階と；ｂ）データ分散選択信号が印加されたか否かを前記個人データ管理アプリケーション６が判断する段階と；ｃ）特定データが選択されたか否かを前記個人データ管理アプリケーション６が判断する段階と；ｄ）前記個人データ管理アプリケーション６がデータ伝送先の情報をデータ管理サーバ１０に要求する段階と；ｅ）前記データ管理サーバ１０がデータ伝送先の情報を前記個人データ管理アプリケーション６に提供する段階と；ｆ）前記個人データ管理アプリケーション６がデータを所定数のデータに分割処理する段階と；ｇ）各分割データをデータ伝送先の端末側とランダムにマッチングさせて伝送する段階と；を含むことを特徴とする。

【０００６】

好ましくは、本発明に係る個人データの管理方法において、前記ｅ）段階は前記データ管理サーバ１０が格納先となる端末識別情報プール（Ｐｏｏｌ）から所定数の識別情報をランダムに抽出する段階を更に含む。

【０００７】

好ましくは、本発明に係る個人データの管理方法において、前記ｆ）段階は前記個人データ管理アプリケーション６が前記データ管理サーバ１０から提供されたデータ伝送先の端末のうち一部をランダムに抽出することによって、最終伝送先の端末を決定する段階を更に含む。

【０００８】

好ましくは、本発明に係る個人データの管理方法において、前記ｇ）段階は前記個人データ管理アプリケーション６が分割されたバックアップデータを別のデータバックアップ先の端末に伝送する段階を更に含む。

【０００９】

好ましくは、本発明に係る個人データの管理方法において、前記ｇ）段階の後に、ｈ）前記個人データ管理アプリケーション６がデータ復旧モードが選択されたか否かを判断する段階と；ｉ）特定データ復旧信号が受信されると、前記個人データ管理アプリケーション６がデータの分割データを分散格納する格納先端末情報を抽出する段階と；ｊ）前記個人データ管理アプリケーション６がデータの格納先端末にデータ伝送要求の処理を行って、データを受信する段階と；ｋ）データの受信が完了すると、前記個人データ管理アプリケーション６がデータを復旧する段階を更に含む。

【００１０】

好ましくは、本発明に係る個人データの管理方法において、前記ｋ）段階は、前記個人データ管理アプリケーション６がデータの格納先端末にデータ伝送を要求した時点から一部の端末から一定時間の経過時までデータが受信されないと、前記個人データ管理アプリケーション６がデータのバックアップ格納先の端末情報を抽出する段階と；前記個人データ管理アプリケーション６がバックアップ格納先の端末側にデータ伝送要求の処理を行う段階を更に含む。

【００１１】

好ましくは、本発明に係る個人データの管理方法において、前記ｇ）段階の後に、前記個人データ管理アプリケーション６が前記データ管理サーバ１０にデータ伝送先の端末情報を伝送する段階を更に含む。

【００１２】

好ましくは、本発明に係る個人データの管理方法において、前記ｈ）段階とｉ）段階と

の間には、ｌ）前記個人データ管理アプリケーション６が復旧するデータ情報を前記データ管理サーバ１０に伝送し、データの認証ユーザ情報を要求する段階と；ｍ）前記データ管理サーバ１０がデータの認証ユーザ情報を個人データ管理アプリケーション６に伝送する段階と；ｎ）前記個人データ管理アプリケーション６が認証ユーザ端末２に個人認証情報の入力を要求する段階と；ｏ）認証ユーザ端末２で個人認証成功時に認証ユーザのユーザ端末２は前記個人データ管理アプリケーション６に認証確認信号を伝送する段階を更に含む。

【００１３】

好ましくは、本発明に係る個人データの管理方法において、前記ｍ）段階は前記データ管理サーバ１０がショートメッセージや電子メールを通じて認証ユーザ情報を個人データ管理アプリケーション６に伝送する段階である。

【００１４】

好ましくは、本発明に係る個人データの管理方法において、前記ｏ）段階は認証失敗信号が前記認証ユーザ端末２から受信されると、前記個人データ管理アプリケーション６は前記データ管理サーバ１０に認証失敗情報を伝送する段階と；前記個人データ管理アプリケーション６が認証ユーザ端末２に個人認証情報の入力を要求した時点から所定時間の経過時まで認証信号が受信されないと、個人データ管理アプリケーション６は前記データ管理サーバ１０に新規な認証ユーザ情報を要求する信号を伝送する段階と；前記データ管理サーバ１０が個人データ管理アプリケーション６に新規な認証ユーザ情報を伝送する段階を更に含む。

【００１５】

好ましくは、本発明に係る個人データの管理方法において、前記ｋ）段階は前記個人データ管理アプリケーション６がデータの格納先端末にデータ伝送を要求した時点から所定時間の経過時まで特定の分割データが受信されたか否かを判断する段階と；特定の分割データが受信されない時、バックアップデータを格納するユーザ端末情報を抽出する段階と；前記個人データ管理アプリケーション６がバックアップデータを格納するユーザ端末２側にデータ伝送を要求する段階を更に含む。

【００１６】

好ましくは、本発明に係る個人データの管理方法において、データを分割して伝送する伝送ユーザ端末２－１と、分割格納したデータを復旧しようとする受信ユーザ端末２－３が互いに異なる場合、格納ユーザ端末（２ａ）は前記受信ユーザ端末２－３側に伝送ユーザ端末２－１により分割されて格納されるデータと、受信認証情報と、残りの分割データの格納端末情報を伝送する段階を更に含む。

【００１７】

また、前述した目的を達成するための本発明に係る個人データ管理システムは、ユーザ認証により駆動され、ユーザが選択した特定データを複数のデータに自動分離して、データ管理サーバ１０から伝送された特定識別番号の複数の第２ユーザ端末２－２に分散して伝送し、ユーザの復旧指令に応じて分散データをまとめて復旧させる個人データ管理アプリケーション６がインストールされた第１ユーザ端末２－１と；前記個人データ管理アプリケーション６がインストールされた第１ユーザ端末２－１の識別情報を格納し、前記第１ユーザ端末２－１からデータの分散信号を受けて、データの分散格納先となる特定のユーザ端末識別情報を抽出して前記第２ユーザ端末２－２に伝送処理するデータ管理サーバー１０と；を含むことを特徴とする。

【００１８】

好ましくは、本発明に係る個人データ管理システムにおいて、前記データ管理サーバ１０は特定のユーザ端末識別情報を抽出する際、格納先となる端末識別情報プール（Ｐｏｏｌ）から所定数の識別情報をランダムに抽出するように構成される。

【００１９】

好ましくは、本発明に係る個人データ管理システムにおいて、前記個人データ管理アプリケーション６は前記データ管理サーバ１０から提供されたユーザ端末識別情報のうち所

定数の識別情報をランダムに抽出するように構成される。

【００２０】

好ましくは、本発明に係る個人データ管理システムにおいて、データを分散して伝送する前記第１ユーザ端末２－１と、データを分散して伝送する前記第２ユーザ端末２－２と、前記データ管理サーバ１０との間に伝送されるデータは暗号化されたデータである。

【００２１】

好ましくは、本発明に係る個人データ管理システムにおいて、前記個人データ管理アプリケーション６は複数に分割されたデータのうちいずれかのデータを第１ユーザ端末２－１に格納し、それ以外のデータは特定識別番号の複数の第２ユーザ端末２－２に分散して格納するように構成される。

【００２２】

好ましくは、本発明に係る個人データ管理システムにおいて、前記個人データ管理アプリケーション６は、その内部に、データを分散格納する複数の第２ユーザ端末２－２及びデータ管理サーバ１０と通信する通信モジュール２０と、個人識別情報の認証を通じてユーザを認証するユーザ認証部２２と、前記データ管理サーバ１０にデータを分散格納する格納先情報を自動で要求する格納先情報要求部２４と；ユーザが選択した特定データを分割処理するデータ分割処理部２８と、通信データの暗号化及び復号化を行う暗号／復号処理部３２と；分割処理したデータのうち一部のデータを格納し、各分割処理したデータが格納されている格納先情報を格納するデータ格納部３４と、前記データ管理サーバ１０と通信してデータ格納先情報の提供を受け、特定データを分割して一部のデータは格納し、それ以外のデータは複数のデータ格納先端末に伝送して分散格納するように処理し、データの復旧時に格納先端末側に特定データの伝送要求信号を伝送して復旧を行う制御部３６と、を含む。

【００２３】

好ましくは、本発明に係る個人データ管理システムにおいて、前記個人データ管理アプリケーション６は、その内部に、前記データ管理サーバ１０から受信した格納先情報のうち一部をランダムに抽出する格納先ランダム抽出部２６を更に含む。

【００２４】

好ましくは、本発明に係る個人データ管理システムにおいて、前記個人データ管理アプリケーション６は、その内部に、分割されたデータとデータの格納先とがランダムにマッチングされるように処理する格納先ランダムマッチング部３０を更に含む。

【００２５】

好ましくは、本発明に係る個人データ管理システムにおいて、前記個人データ管理アプリケーション６は複数のデータ伝送先の端末に分割データを伝送し、同じ分割データをバックアップ先の端末側に伝送してバックアップ格納するように処理し、データの復旧時に一定時間内に特定の分割データの復旧が行われないと、バックアップデータを用いた復旧処理を行うように構成される。

【００２６】

好ましくは、本発明に係る個人データ管理システムにおいて、前記データ管理サーバ１０は特定データの復旧時に認証が必要な単一の認証ユーザ情報をデータ分散格納時に登録し、前記個人データ管理アプリケーション６のデータ復旧要求時に、認証ユーザ情報を個人データ管理アプリケーション６に提供するように構成される。

【００２７】

好ましくは、本発明に係る個人データ管理システムにおいて、前記個人データ管理アプリケーション６は前記データ管理サーバ１０から認証ユーザ情報が提供されると、認証ユーザのユーザ端末２側に個人認証情報の入力を要求するように構成され、個人認証成功時に認証ユーザの第３ユーザ端末２－３は前記個人データ管理アプリケーション６に認証確認信号を伝送するように構成される。

【００２８】

好ましくは、本発明に係る個人データ管理システムにおいて、前記データ管理サーバ１

０が前記個人データ管理アプリケーション６に伝送する認証ユーザ情報はテキストメッセージや電子メールを通じて伝送するように構成される。

【００２９】

好ましくは、本発明に係る個人データ管理システムにおいて、前記個人データ管理アプリケーション６は、前記個人データ管理アプリケーション６が認証ユーザ端末２に個人認証情報の入力を要求した時点から所定時間の経過時まで認証ユーザの認証確認情報が受信されないと、前記データ管理サーバ１０に新規な認証ユーザ情報を要求するように構成される。

【００３０】

好ましくは、本発明に係る個人データ管理システムにおいて、前記ユーザ端末は元データを分割する第１伝送ユーザ端末２－１と、元データを復旧する第３ユーザ端末２－３が互いに異なって構成される場合、前記第１ユーザ端末２－１は受信ユーザ端末２－３に第１ユーザ端末２－１により分割されて格納されるデータと、受信認証情報と、残りの分割データの格納端末情報を伝送するように構成される。

【００３１】

好ましくは、本発明に係る個人データ管理システムにおいて、分散データを格納する前記複数の第２ユーザ端末２－２はサーバ、ＰＣ、及び無線端末のうちいずれか一つである。

【発明の効果】

【００３２】

本発明に係る個人データ管理システム及びその方法によれば、個人データを分割して複数のユーザ端末に分散格納することによって、データ管理サーバやメールサーバ、またはＳＮＳサーバーがハッキングを受けても、データの流出を完全に防止するか、ハッキングの成功時にも分割データの一部のみが流出してハッキングの意味がなく、サーバーがハッキングを受けても、複数の第２ユーザ端末をハッキングしていないと、全ての分割データを得ることができない。また、特定データに関連した複数のユーザ端末をハッキングしても、最終的に一人の個人の特定データのみが流出するので、ハッカーの実益が非常に少なく、セキュリティ性能が強化できる長所がある。

【図面の簡単な説明】

【００３３】

【図１】本発明の第１実施形態に係る個人データ管理システムの構成を示す模式図

【図２】本発明の第１実施形態に係る個人データ管理システムを用いたデータの格納先選定の状態を示す説明図

【図３】本発明の第１実施形態に係る個人データ管理システムを用いたデータの分割格納及び復旧の状態を示す説明図

【図４】本発明の第１実施形態に係る個人データ管理システムに含まれた個人データ管理アプリケーションの駆動を示すブロック構成図

【図５】本発明の第１実施形態に係る個人データ管理システムの信号の流れを示すフローチャート

【図６】本発明の第２実施形態に係る個人データ管理システムの構成を示す模式図

【図７】本発明の第２実施形態に係る個人データ管理システムの構造を示す概念図

【図８】本発明の第２実施形態に係る個人データ管理システムを用いた認証対象ユーザの選定状態を示す説明図

【図９】本発明の第２実施形態に係る個人データ管理システムを用いたデータ復旧プロセスを示すフローチャート

【図１０】図９に続くデータ復旧プロセスを示すフローチャート

【図１１】図１０に続くデータ復旧プロセスを示すフローチャート

【図１２】本発明の第３実施形態に係る個人データ管理システムの構成を示す模式図

【発明を実施するための最良の形態】

【００３４】

以下、本発明の第１実施形態に係る個人データ管理システムについて添付図面を参照して詳細に説明する。

図１は本発明の第１実施形態に係る個人データ管理システムの構成を示す模式図であり、図２は本発明の第１実施形態に係る個人データ管理システムを用いたデータの格納先選定の状態を示す図であり、図３は本発明の第１実施形態に係る個人データ管理システムを用いたデータの分割格納及び復旧の状態を示す図である。

【００３５】

これらの図を参照すれば、本発明の第１実施形態に係る個人データ管理システムは、ユーザの個人データをユーザ端末や特定サーバーに格納せずにランダムに分散格納して管理し、必要に応じて複数の認証手続きを経てユーザ端末で個人データを復旧することによって、ハッキングを受ける可能性が大幅に低減すると共に、ユーザ端末の紛失時にもデータの流出を防止できるシステムである。

即ち、本発明の第１実施形態に係る個人データ管理システムは、いずれかの記憶媒体にユーザが格納しようとするデータの全体を一括して格納せずに全体のデータを複数に分割して分散格納させることによって、いずれかの格納手段がハッキングを受けても、データが流出する恐れがないシステムである。

【００３６】

より詳細には、本発明の第１実施形態に係る個人データ管理システムは、ユーザ認証により駆動され、ユーザが選択した特定データを複数のデータに自動分離して、データ管理サーバ１０から伝送された特定識別番号の複数のユーザ端末２に分散して伝送し、ユーザの復旧指令に応じて、分散データをまとめて復旧させる個人データ管理アプリケーション６がインストールされたユーザ端末２と；個人データ管理アプリケーション６がインストールされたユーザ端末の識別情報を格納し、ユーザ端末２からデータの分散信号を受けて、データの分散格納先となる特定のユーザ端末識別情報を抽出して、ユーザ端末２に伝送処理するデータ管理サーバ１０と；からなる。

この時、ユーザ端末２は分割前の元データ４を格納しており、実際に元データ４を分割し、分割されたデータを別の記憶媒体に伝送し、再分割されたデータを元データ４に復旧させるデータ分割及び復旧用のユーザ端末２と；ユーザ端末２から伝送される分割データ８を格納する格納用のユーザ端末２に区分できる。

即ち、これらのユーザ端末２は、その内部に個人データ管理アプリケーション６をインストールすることで、データの分割及び伝送を行うことができ、分割されたデータを受信して格納することもでき、分割されたデータを復旧することもできる。

【００３７】

従って、ユーザ端末２はあえてその機能に応じた区分する必要がないが、説明の便宜上、データを分割して伝送し、再分割されたデータを復旧させるユーザ端末２には別のコード（例、Ａ００１）を与え、分割されたデータの伝送を受けてそれぞれ格納するユーザ端末２にも別のコード（例、Ｂ００１、Ｃ００１、Ｄ００１、Ｅ００１）を与えて示す。

そして、以下には説明の便宜のためにＡ００１のコードが与えられたユーザ端末２を第１ユーザ端末２－１と称し、Ｂ００１－Ｅ００１のコードが与えられたユーザ端末２は第２ユーザ端末２－２と称する。

【００３８】

一方、データ管理サーバ１０は特定のユーザ端末識別情報を抽出する際、格納先となる端末識別情報プール（Ｐｏｏｌ）から所定数の識別情報をランダムに抽出するように構成される。

即ち、第１ユーザ端末２－１がデータを分割して格納しようとする格納先に関する情報をデータ管理サーバ１０に要求すると、データ管理サーバ１０は予め分割データを格納することができる格納先に関する情報を抽出して第１ユーザ端末２－１に伝送する。

従って、データ管理サーバ１０は分割データを格納する格納先に関する情報を格納している。ここで、格納先とは第２ユーザ端末２－２を意味する。

【００３９】

また、データ管理サーバ１０は複数の分割データ伝送先の端末である第２ユーザ端末２－２の識別情報を格納している。複数の第２ユーザ端末２－２のうち一部の第２ユーザ端末２－２の識別情報をランダムに抽出して第１ユーザ端末２－１側に提供する。

好ましく、第１ユーザ端末２－１の個人データ管理アプリケーション６はデータ管理サーバ１０から提供されたユーザ端末識別情報のうち所定数の識別情報をランダムに抽出するように構成される。

即ち、データ管理サーバ１０は第２ユーザ端末２－２の識別情報をランダムに抽出して、第１ユーザ端末２－１に提供したものと同様に、第１ユーザ端末２－１もデータ管理サーバ１０から提供された識別情報のうち一部の第２ユーザ端末２－２の識別情報をランダムに抽出し、その抽出情報をデータ管理サーバ１０に伝送する。

これによって、本発明の第１実施形態に係る個人データ管理システムに含まれるデータの管理サーバー１０は、第１ユーザ端末２－１が格納しようとするいずれかの分割データを格納せずに、単に分割データがどの端末に格納されているかに関する情報のみを保持する。従って、ハッカーによって不法にハッキングされてもハッカーがユーザのデータを取得することができない。

【００４０】

一方、第１ユーザ端末２－１は、例えば、全体の元データ４のうち分割された一部の分割データ（８：例えば、Ｄ－１）を格納しており、複数の分割データを格納している格納先となる第２ユーザ端末２－２（例えば、Ｂ００１、Ｃ００１、Ｄ００１、Ｅ００１．．．）の識別情報のみを格納しているので、ハッカーのハッキングを受けても、ユーザが隠したいデータの一部分割データのみを取得することができる。

即ち、第１ユーザ端末２－１にインストールされた個人データ管理アプリケーション６は複数に分割されたデータのうちいずれかのデータは第１ユーザ端末２－１に格納し、それ以外のデータは特定識別番号の複数のユーザ端末２、即ち第２ユーザ端末２－２に分散して格納するように構成される。

この時、分散データを格納する複数の第２ユーザ端末２－２はサーバやＰＣ、または無線端末のうちいずれか一つである。

【００４１】

また、元データ４を分割して格納するいずれかの第２ユーザ端末２－２（例えば、Ｂ００１）には、いずれかの一部の分割データ（８：例えば、Ｄ－３）を格納しており、いずれかの第２ユーザ端末２－２（例えば、Ｃ００１）には、いずれかの一部の分割データ（８：例えば、Ｄ－２）を格納しており、いずれかの第２ユーザ端末２－２（例えば、Ｄ００１）には、いずれかの一部の分割データ（８　：例えば、Ｄ－５）を格納しており、いずれかの第２ユーザ端末２－２（例えば、Ｅ００１）には、いずれかの一部の分割データ（８：例えば、Ｄ－４）を格納しているので、同様に、いずれかの第２ユーザ端末２がハッキングを受けても、一部の分割データのみを確保することができる。

特に、通常は、いずれかのサーバーに複数のユーザデータが格納されているため、ハッキング時のハッキングに係る労力に対する対価が得られるが、本発明では、データ管理サーバ１０をハッキングしても、ハッカーが得ることができる元データ４が全く格納されておらず、いずれかの一人の個人データを取得するためには無数のユーザ端末２をハッキングしなければならない。そのため、現実的にはハッカーが得ることができる代価がほとんどなくなる。

【００４２】

一方、一般的な通信データの送受信時と同様に、本発明の第１実施形態に係る個人データ管理システムにおけるデータは、データを分散して伝送するユーザ端末２とデータ管理サーバ１０との間に伝送される暗号化されたデータである。

一方、好ましく、本発明の第１実施形態に係る個人データ管理システムは、いずれかの第２ユーザ端末２－２を紛失したか、または応答できない場合を想定して、データをバックアップする構造に設計した。

即ち、第１ユーザ端末２－１にインストールされた個人データ管理アプリケーション６

は、複数のデータ伝送先の端末、例えば、第２ユーザ端末２－２に分割データを伝送し、同じ分割データをバックアップ先である他の第２ユーザ端末２－２側に伝送してバックアップ格納するように処理する。データの復旧時には、一定時間内に特定の分割データの復旧が行われないと、バックアップデータを用いた復旧処理を行うように構成する。

従って、第１ユーザ端末２－１にインストールされた個人データ管理アプリケーション６は、分割データを格納する第２ユーザ端末２－２の識別情報と、バックアップデータを格納する第２ユーザ端末２－２の識別情報をそれぞれ格納している。

【００４３】

図４は本発明の第１実施形態に係る個人データ管理システムに含まれた個人データ管理アプリケーションの駆動を示すブロック構成図である。

これらの図を参照すれば、個人データ管理アプリケーション６は、その内部に、データを分散格納する複数のユーザ端末２及びデータ管理サーバ１０と通信する通信モジュール２０と、個人識別情報の認証を通じてユーザを認証するユーザ認証部２２と、データ管理サーバ１０にデータを分散格納する格納先情報を自動で要求する格納先情報要求部２４を含んで構成される。

また、個人データ管理アプリケーション６は、その内部に、ユーザが選択した特定データを分割処理するデータ分割処理部２８と、通信データの暗号化及び復号化を行う暗号／復号処理部３２と；分割処理したデータのうち一部のデータを格納し、各分割処理したデータが格納されている格納先情報を格納するデータ格納部３４と、データ管理サーバ１０と通信してデータ格納先情報の提供を受け、特定データを分割して一部のデータは格納し、それ以外のデータは複数のデータ格納先端末に伝送して分散格納するように処理し、データの復旧時に格納先端末側に特定データの伝送要求信号を伝送して復旧を行う制御部３６を含んで構成される。

【００４４】

一方、個人データ管理アプリケーション６は、その内部に、データ管理サーバ１０から受信した格納先情報のうち一部をランダムに抽出する格納先ランダム抽出部２６を更に含んで構成される。

また、個人データ管理アプリケーション６は、その内部に、分割されたデータとデータの格納先とがランダムにマッチングされるように処理する格納先ランダムマッチング部３０を更に含んで構成される。

【００４５】

次に、前述した構成の本発明の第１実施形態に係る個人データ管理システムの機能及び作用について添付図面を参照して詳細に説明する。

図５は本発明の第１実施形態に係る個人データ管理システムの信号の流れを示すフローチャートである。

まず、本発明の第１実施形態に係る個人データ管理システムに含まれたユーザ端末２、例えば、第１ユーザ端末２－１を所有しているユーザが特定データを分散格納するために、個人データ管理アプリケーション６を駆動し、パスワードなどの個人認証情報を入力して認証を行う。

認証が成功すると、個人データ管理アプリケーション６はデータ分散モードが選択されたか否かを判断する。

データ分散モードが選択された場合、個人データ管理アプリケーション６は特定データの分散選択信号が印加されたか否かを判断する。

特定データが選択されると、個人データ管理アプリケーション６はデータ伝送先の情報をデータ管理サーバ１０に要求する。

即ち、分割されたデータを格納するための格納先の識別情報をデータ管理サーバ１０に要求すると、データ管理サーバ１０は複数の分割データ伝送先の端末である第２ユーザ端末２－２の識別情報を格納している。複数の第２ユーザ端末２－２のうち一部の第２ユーザ端末２－２の識別情報をランダムに抽出して、第１ユーザ端末２－１の個人データ管理アプリケーション６に提供する。

【００４６】
その後、個人データ管理アプリケーション６は、更にデータ管理サーバ１０から提供されたデータ伝送先の端末のうち一部をランダムに抽出することによって、最終伝送先の端末を決定する。
そして、個人データ管理アプリケーション６はデータを所定数のデータに分割処理し、各分割データをデータ伝送先の端末である第２ユーザ端末２－２とランダムにマッチングさせて伝送する。
この時、個人データ管理アプリケーション６は、分割されたバックアップデータを別のデータバックアップ先の端末に伝送する。
即ち、第１ユーザ端末２－１にインストールされた個人データ管理アプリケーション６は複数のデータ伝送先の端末、例えば、第２ユーザ端末２－２に分割データを伝送し、同じ分割データをバックアップ先であるまた他の第２ユーザ端末２－２側に伝送してバックアップ格納するように処理する。
【００４７】
一方、第１ユーザ端末２－１にインストールされた個人データ管理アプリケーション６はデータ復旧モードが選択されたか否かを判断する。この時、特定データ復旧信号が受信されると、個人データ管理アプリケーション６はデータの分割データを分散格納する格納先端末情報、例えば、第２ユーザ端末２－２の識別情報を抽出する。
そして、第１ユーザ端末２－１の個人データ管理アプリケーション６はデータの格納先の端末、例えば、第２ユーザ端末２－２にデータ伝送要求の処理を行う。
複数の分割データの受信が完了すると、個人データ管理アプリケーション６は元データを復旧する。
この時、一部の第２ユーザ端末２－２から、前記個人データ管理アプリケーション６がデータの格納先端末にデータ伝送を要求した時点から一定時間の経過時までデータが受信されないと、個人データ管理アプリケーション６はデータのバックアップ格納先の端末情報を抽出する。
この時、一部の第２ユーザ端末２－２から一定時間の経過時までデータが受信されないと、個人データ管理アプリケーション６はデータのバックアップ格納先の端末情報を抽出する。
そして、個人データ管理アプリケーション６はバックアップ格納先の端末側にデータ伝送要求の処理を行って、元データ４を復旧する。
【００４８】
以下、本発明の第２実施形態に係る個人データ管理システムについて添付図面を参照して詳細に説明する。
図６は本発明の第２実施形態に係る個人データ管理システムの構成を示す模式図であり、図７は本発明の第２実施形態に係る個人データ管理システムの構造を示す概念図であり、図８は本発明の第２実施形態に係る個人データ管理システムを用いた認証対象ユーザの選定状態を示す図である。
これらの図を参照すれば、本発明の第２実施形態に係る個人データ管理システムは、第１実施形態に加えて、オフライン認証プロセスを含むシステムである。
オフライン認証を含む本発明の第２実施形態に係る個人データ管理システムは、第１ユーザ端末２－１からデータ復旧を試みる場合、追加の認証プロセスを更に含んでいるものであって、第１ユーザ端末２－１で分割されたいずれかの分割データ８を格納している第２ユーザ端末２－２のうちいずれかの端末でユーザ認証を行う認証処理を行うようにしたシステムである。
【００４９】
即ち、本発明の第２実施形態に係る個人データ管理システムは、第１ユーザ端末２－１から特定データの復旧を試みると、いずれかの第２ユーザ端末２－２のユーザ認証を、その第２ユーザ端末２－２にインストールされた個人データ管理アプリケーション６が行い、その認証成功信号を第１ユーザ端末２－１の個人データ管理アプリケーション６に伝送

した後に、 第１ユーザ端末２－１の個人データ管理アプリケーション６がデータの復旧を指令するように構成される。

この時、認証対象となる特定の第２ユーザ端末２－２の所有者を認証ユーザと称し、データ管理サーバ１０は第１ユーザ端末２－１を通じて分割された特定データの識別情報にマッチングされるように、認証ユーザの情報を乱数処理モジュール１２を通じてランダムに生成させて格納する。

【００５０】

また、その認証ユーザの情報の場合、第１ユーザ端末２－１には格納されていないため、ハッカーが第１ユーザ端末２－１をハッキングしてデータを復旧しようとしても、認証ユーザ情報がなければデータ復旧が行われない。

即ち、データ管理サーバ１０は特定データの復旧時に認証が必要な単一の認証ユーザ情報をデータ分散格納時に登録し、第１ユーザ端末２－１の個人データ管理アプリケーション６はデータ復旧を要求すると、認証ユーザ情報を個人データ管理アプリケーション６に提供する。

従って、第１ユーザ端末２－１の個人データ管理アプリケーション６はデータ管理サーバ１０から認証ユーザ情報が提供されると、認証ユーザのユーザ端末２（例えば、第２ユーザ端末２－１）側に個人認証情報（例えば、パスワードや指紋、虹彩情報など）の入力を要求するように構成され、個人認証成功時に認証ユーザの第２ユーザ端末２－２は第１ユーザ端末２－１の個人データ管理アプリケーション６に認証確認信号を伝送する。

特に、本発明の第２実施形態に係る個人データ管理システムにおいては、データ管理サーバ１０がテキストメッセージや電子メールを通じて認証ユーザ情報を個人データ管理アプリケーション６に伝送するように構成される。

【００５１】

そのため、本発明の第２実施形態に係る個人データ管理システムは、オフラインの概念を加えて、異種通信の概念を含む。データ管理サーバ１０から第１ユーザ端末２－１に認証ユーザの識別情報を伝送する際、第１ユーザ端末２－１を所有しているユーザの電子メールでその認証ユーザの識別情報を伝送する。その場合、ハッカーがたとえ第１ユーザ端末２－１の個人データ管理アプリケーション６のパスワードを知っていても、ユーザの電子メール伝送サーバー４０をハッキングしていなければデータを復旧させることができない。

一方、認証ユーザの対象となった特定の第２ユーザ端末２－２はユーザの認証情報の入力を通じて個人データ管理アプリケーション６のユーザ認証が成功しなければならない。しかし、一定時間が経過するように、認証ユーザの認証成功信号が第１ユーザ端末２－１の個人データ管理アプリケーション６に受信されない場合もある。

その場合、個人データ管理アプリケーション６は所定時間の経過時まで認証ユーザの認証確認情報が受信されないと、データ管理サーバ１０に新規な認証ユーザ情報を要求するように構成されることも可能である。

【００５２】

次に、前述した構成の本発明の第２実施形態に係る個人データ管理システムの機能及び作用について添付図面を参照して詳細に説明する。

図９、１０、１１は本発明の第２実施形態に係る個人データ管理システムを用いたデータ復旧プロセスを示すフローチャートである。

まず、本発明の第２実施形態に係る個人データ管理システムは、分割して遠隔地に分散格納した分割データを復旧する過程で、特定のユーザの認証を行うオフライン認証の概念と、異種通信の概念を更に含むものである。

【００５３】

ここで、オフライン認証の概念とは、特定のユーザが直接パスワードを入力するか、または指紋や虹彩などの情報を入力してユーザ認証を行うようにしたものであって、個人データの管理会員に登録してユーザ端末２に個人データ管理アプリケーション６がインストールされたユーザであれば誰でも認証ユーザの対象となることができる。その認証ユーザ

はデータ管理サーバ１０がランダムに指定する。
認証ユーザの指定の場合は、第１ユーザ端末２－１からデータ復旧要求がある時点でデータ管理サーバ１０が行うようになる。
好ましく、第１ユーザ端末２－１は特定データの分割データを格納している複数の第２ユーザ端末２－２の識別情報を格納することもできるが、第１ユーザ端末２－１は情報をデータ管理サーバ１０に伝送して格納し、第１ユーザ端末２－１にはデータの格納先端末である第２ユーザ端末２－２の情報を削除することもできる。
この時、情報を削除した状態であれば、データの復旧時に第１ユーザ端末２－１の個人データ管理アプリケーション６はデータ管理サーバ１０に復旧しようとする特定データの識別情報（例えば、Ｐｉｇ２０１３）を伝送すると同時に、認証ユーザの識別情報を要求する。

【００５４】
その後、データ管理サーバ１０はアプリケーション６がインストールされた第２ユーザ端末２－２を有しているいずれかのユーザの識別情報（例えば、電話番号）を抽出して、第１ユーザ端末２－１の個人データ管理アプリケーション６に伝送する。
この時、好ましく、本発明の第２実施形態に係る個人データ管理システムは、オフラインの概念を加えて、異種通信の概念を含む。従って、データ管理サーバ１０から認証ユーザの識別情報を第１ユーザ端末２－１に伝送する際に、第１ユーザ端末２－１を所有しているユーザの電子メールでその認証ユーザの識別情報を伝送する。その場合、ハッカーがたとえ第１ユーザ端末２－１の個人データ管理アプリケーション６のパスワードを知っていてもユーザの電子メールサーバ４０をハッキングしていなければデータを復旧させることができない。

【００５５】
次に、第１ユーザ端末２－１の個人データ管理アプリケーション６は認証ユーザの識別情報を有している第２ユーザ端末２－２に認証要求信号を伝送する。この時、好ましく、認証要求信号を第２ユーザ端末２－２の個人データ管理アプリケーション６に伝送する。
それによって、第２ユーザ端末２－２を所有しているユーザは第２ユーザ端末２－２の個人データ管理アプリケーション６に認証情報を入力して認証を行うようにする。この時、好ましく、個人データ管理アプリケーション６のパスワードを入力すればよい。
パスワード認証が成功すると、第２ユーザ端末２－２の個人データ管理アプリケーション６は第１ユーザ端末２－１の個人データ管理アプリケーション６に認証成功信号を伝送する。

【００５６】
その後、第１ユーザ端末２－１の個人データ管理アプリケーション６は分割データを格納する複数の第２ユーザ端末２－２にデータ復旧信号を伝送する。好ましく、復旧しようとするデータの識別情報も共に伝送する。
それによって、第２ユーザ端末２－２の個人データ管理アプリケーション６は分割データ８を第１ユーザ端末２－１に伝送する。
第１ユーザ端末２－１の個人データ管理アプリケーション６は分割されたデータが全て受信したか否かを判断し、分割データの受信が完了すると、データを復旧する。
それに対して、第２ユーザ端末２－２の個人データ管理アプリケーション６が個人認証情報を入力したが、パスワードの不一致などにより個人認証に失敗した場合は、第２ユーザ端末２－２の個人データ管理アプリケーション６は第１ユーザ端末２－１の個人データ管理アプリケーション６に、認証失敗情報を伝送し、第１ユーザ端末２－１の個人データ管理アプリケーション６は再びデータ管理サーバ１０に認証ユーザの認証失敗情報を伝送する。

【００５７】
また、一定時間が経過する時点まで第１ユーザ端末２－１に認証成功信号が受信されない場合もある。
その場合にも、同様に、第１ユーザ端末２－１の個人データ管理アプリケーション６は

データ管理サーバ１０に認証信号未受信に関する情報を伝送することができる。いずれの場合も、データ管理サーバ１０が新規な認証ユーザの識別情報を要求する。

また、図１１に示すように、認証が成功したが、一定時間が経過する時点まで分割データが第１ユーザ端末２－１の個人データ管理アプリケーション６に受信されない場合は、第１ユーザ端末２－１個人データ管理アプリケーション６が受信されない分割データのバックアップデータを格納した第２ユーザ端末２－２の識別情報を抽出して、第２ユーザ端末２－２の個人データ管理アプリケーション６にバックアップデータの伝送を要求することができる。

【００５８】

一方、バックアップデータを格納した第２ユーザ端末２－２の識別情報をデータ管理サーバ１０に格納し、第１ユーザ端末２－１にはその識別情報を格納しないように設計することもできる。

この場合は、図１１に示すように、第１ユーザ端末２－１の個人データ管理アプリケーション６はデータ管理サーバ１０に受信されない分割データのバックアップデータを要求することができる。

その後、データ管理サーバ１０は分割データのバックアップデータを格納した第２ユーザ端末２－２の識別情報を抽出して、第２ユーザ端末２－２の個人データ管理アプリケーション６にバックアップデータの伝送を要求して受信を受け、受信したバックアップデータを再び第１ユーザ端末２－１に伝送してデータ復旧が行われるようすることができる。

【００５９】

以下、本発明の第３実施形態に係る個人データ管理システムについて添付図面を参照して詳細に説明する。

図１２は本発明の第３実施形態に係る個人データ管理システムの構成を示す模式図である。

この図を参照すれば、本発明の第３実施形態に係る個人データ管理システムは、複数の第２ユーザ端末２－２に格納された第１ユーザ端末（２ａ：以下２－１で説明する）の分割データを第１ユーザ端末２－１の元データ４に復旧せず、第１ユーザ端末２－１が指定した特定の第３ユーザ端末（２ｂ：以下２－３に説明する）に復旧するようにしたシステムである。

これらの機能は電子メールの伝送やＳＮＳを通じて特定データを特定のユーザに伝送する時、データセキュリティの維持に非常に効果的である。

【００６０】

即ち、第１ユーザ端末２－１の個人データ管理アプリケーション６は電子メールを伝送する時に自動で起動されて伝送元データ４を複数のデータに分割し、一部の分割データ（例えば、Ｄ－１）を受信側である第３ユーザ端末２－３の個人データ管理アプリケーション６に直接伝送し、データの閲覧が可能な閲覧認証情報（好ましく、パスワード）を共に伝送する。

そして、第１ユーザ端末２－１の個人データ管理アプリケーション６は残りの分割データを複数の第２ユーザ端末２－２の個人データ管理アプリケーション６に伝送して格納させる。

その状態で、第３ユーザ端末２－３の個人データ管理アプリケーション６にデータの閲覧が可能なパスワードが入力されると、その第３ユーザ端末２－３の個人データ管理アプリケーション６はパスワード情報を第１ユーザ端末２－１の個人データ管理アプリケーション６に伝送する。

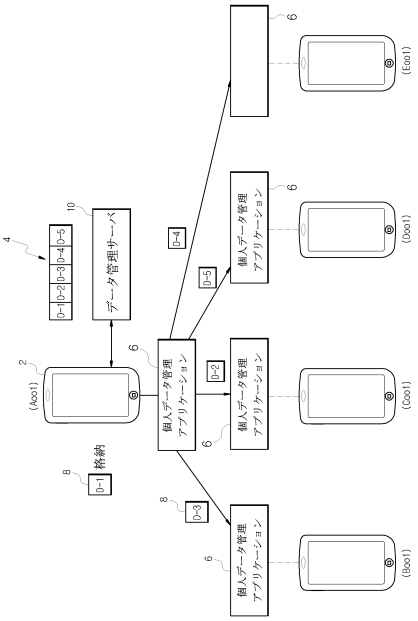
それによって、第１ユーザ端末２－１の個人データ管理アプリケーション６はパスワードを認証して正当なデータ閲覧者であるか否かを認証するようになり、パスワードが一致した場合、第１ユーザ端末２－１の個人データ管理アプリケーション６はデータを分散格納している複数の第２ユーザ端末２－２にデータ伝送送号を発生させる。

【００６１】

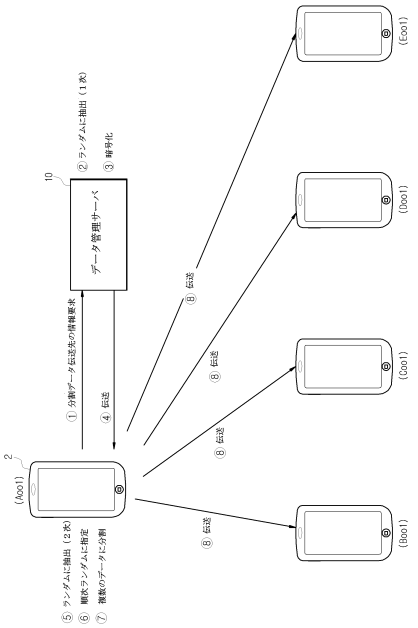
その後、第２ユーザ端末２－２の個人データ管理アプリケーション６は分割データ８を

それぞれ第３ユーザ端末２－３の個人データ管理アプリケーション６に伝送する。
それによって、第３ユーザ端末２－３の個人データ管理アプリケーション６はデータを復旧することができる。
これらの機能は電子メールサーバと連動して動作することができる。
即ち、第１ユーザ端末２－１の個人データ管理アプリケーション６からメール伝送をクリックすると、ユーザが予め指定した電子メールアプリケーション（不図示）を自動で駆動するように、第１ユーザ端末２－１の個人データ管理アプリケーション６で信号を発生させる。
そして、第１ユーザ端末２－１の個人データ管理アプリケーション６は特定データに対して、分割されたいずれかの分割データ（例えば、Ｄ－１）を電子メールに自動で添付させ、パスワードと格納個所情報、例えば、第２ユーザ端末２－２の個人データ管理アプリケーション６の識別情報を電子メールの本文に入力して伝送する。
【００６２】
または、電子メールの代わりにショートメッセージを通じて識別情報を伝送することも可能である。
この時、第１ユーザ端末２－１の個人データ管理アプリケーション６は、電子メールを受信するユーザの電子メール情報と共に受信者の端末である第３ユーザ端末２－３の識別情報、第２ユーザ端末２－２の個人データ管理アプリケーション６の識別情報を共に格納していなければならない。
そして、第１ユーザ端末２－１の個人データ管理アプリケーション６は残りの分割データを第２ユーザ端末２－２に伝送する。
その状態で、第３ユーザが個人データ管理アプリケーション６を通じてデータの復旧命令を第２ユーザ端末２－２の個人データ管理アプリケーション６に発生させると、第２ユーザ端末２－２の個人データ管理アプリケーション６は第３ユーザ端末２－３に分割データを伝送する。
それによって、第３ユーザ端末２－３の個人データ管理アプリケーション６は分割データを受信するようになり、第１ユーザが伝送したパスワードを入力すると、データが画面に出力されるようになる。
【００６３】
従って、本発明においては、電子メール伝送方式に適用する時と同様に、ＳＮＳサーバ（不図示）がハッキングを受けない限り、ハッカーは第１ユーザ端末２－１はＳＮＳを通じて第３ユーザ端末２－３に伝送する分割データを獲得することができない。また、ＳＮＳサーバがハッキングを受けても複数の第２ユーザ端末２－２がハッキング受けない場合は、全ての分割データを得ることができず、各ユーザ端末２がハッキングを受けても、一人の個人の特定データのみを取得できるので、ハッカーには実益がなくなる。
【００６４】
一方、本明細書内で本発明をいくつかの好ましい実施形態によって記述したが、当業者ならば、添付の特許請求範囲に開示した本発明の範疇及び思想から外れずに、多くの変形及び修正がなされ得る。
【符号の説明】
【００６５】
２　ユーザ端末
２－１、２－２、２－３　第１、２、３ユーザ端末
４　元データ
６　個人データ管理アプリケーション
８　分割データ
１０　データ管理サーバ

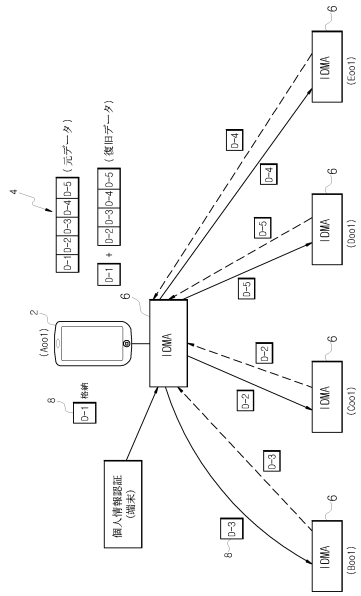
【図１】


データ管理サーバ
10
4
D-1
D-2
D-3
D-4
D-5
2
(Aoo1)
6
個人データ管理
アプリケーション
格納
8
(Boo1)
(Coo1)
(Doo1)
(Eoo1)

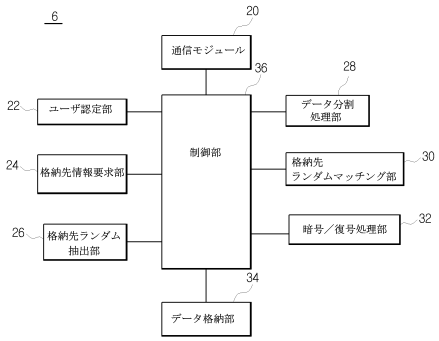
【図２】


データ管理サーバ
10
② ランダムに抽出（1次）
③ 暗号化
① 分割データ伝送先の情報要求
④ 伝送
⑧ 伝送
⑤ ランダムに抽出（2次）
⑥ 順次ランダムに指定
⑦ 複数のデータに分割
2
(Aoo1)
(Boo1)
(Coo1)
(Doo1)
(Eoo1)

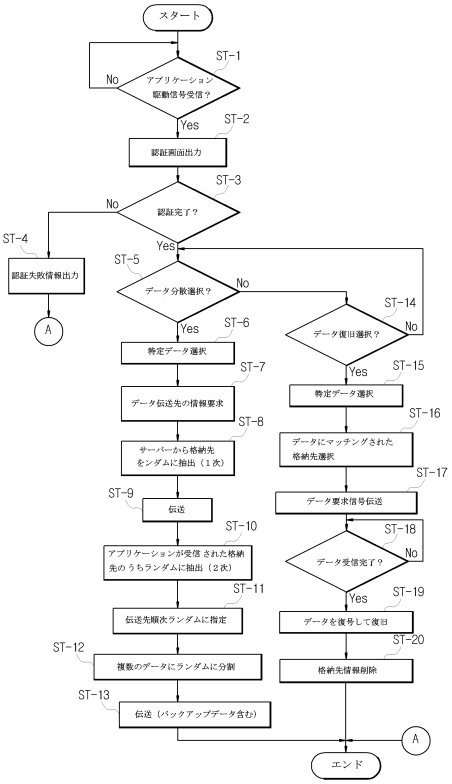
【図３】


4
（元データ）
（復旧データ）
D-1
D-2
D-3
D-4
D-5
2
(Aoo1)
6
IDMA
格納
8
個人情報認証
（端末）
(Boo1)
(Coo1)
(Doo1)
(Eoo1)

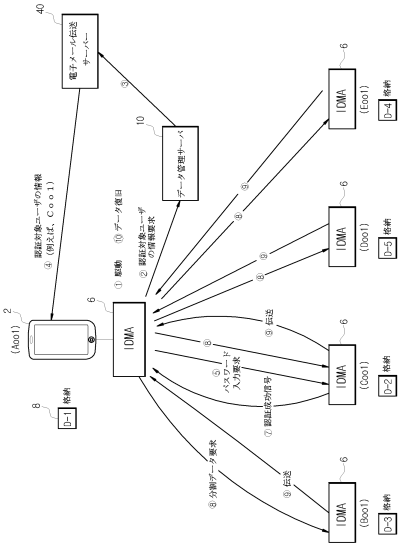
【図４】


6
20
通信モジュール
36
28
22
ユーザ認定部
データ分割
処理部
制御部
24
格納先情報要求部
格納先
ランダムマッチング部
30
26
格納先ランダム
抽出部
暗号／復号処理部
32
34
データ格納部

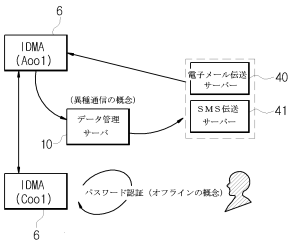
【図５】


スタート
ST-1
アプリケーション駆動信号受信？
No
Yes
ST-2
認証画面出力
ST-3
認証完了？
No
Yes
ST-4
認証失敗情報出力
A
ST-5
データ分散選択？
No
Yes
ST-6
特定データ選択
ST-7
データ伝送先の情報要求
ST-8
サーバーから格納先をンダムに抽出（１次）
ST-9
伝送
ST-10
アプリケーションが受信された格納先のうちランダムに抽出（２次）
ST-11
伝送先順次ランダムに指定
ST-12
複数のデータにランダムに分割
ST-13
伝送（バックアップデータ含む）
ST-14
データ復旧選択？
No
Yes
ST-15
特定データ選択
ST-16
データにマッチングされた格納先選択
ST-17
データ要求信号伝送
ST-18
データ受信完了？
No
Yes
ST-19
データを復号して復旧
ST-20
格納先情報削除
A
エンド

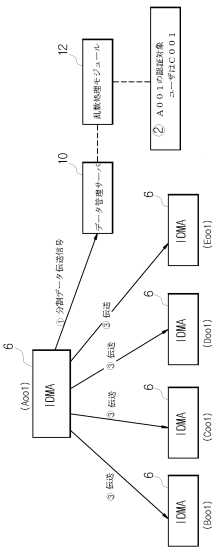
【図６】


40
電子メール伝送サーバー
10
データ管理サーバ
2
(Aoo1)
6
IDMA
8
D-1
格納
(Eoo1)
D-4
(Doo1)
D-3
(Coo1)
D-2
① 配信
② 認証対象ユーザの情報要求
③ 伝送
④ 認証対象ユーザの情報（例えば（Coo1））
⑤ パスワード入力要求
⑥ パスワード入力
⑦ 認証成功信号
⑧ 分割データ要求
⑨ 伝送
⑩ データ復旧

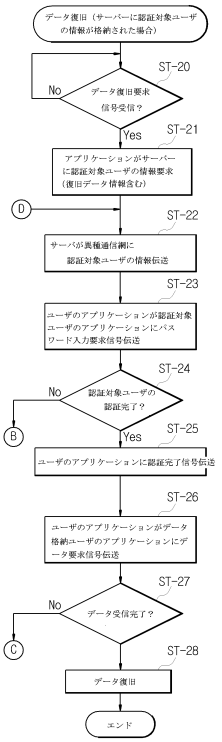
【図７】


6
IDMA
(Aoo1)
電子メール伝送サーバー
40
(異種通信の概念)
データ管理サーバ
10
SMS伝送サーバー
41
IDMA
(Coo1)
6
パスワード認証（オフラインの概念）

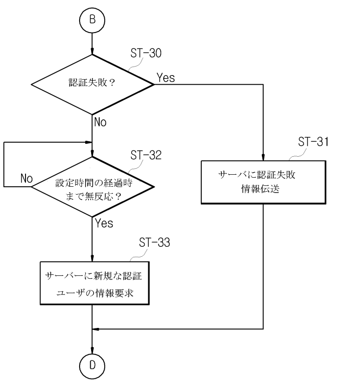
【図８】


12
乱数処理モジュール
② A001の認証対象ユーザはC001
10
データ管理サーバ
① 分割データ伝送指令
6
IDMA
(Aoo1)
③ 伝送
IDMA
(Eoo1)
IDMA
(Doo1)
IDMA
(Coo1)
IDMA
(Doo1)

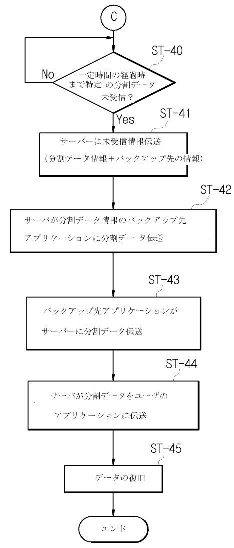
【図９】


データ復旧（サーバーに認証対象ユーザの情報が格納された場合）
ST-20
No
データ復旧要求信号受信？
Yes
ST-21
アプリケーションがサーバーに認証対象ユーザの情報要求（復旧データ情報含む）
D
ST-22
サーバが異種通信網に認証対象ユーザの情報伝送
ST-23
ユーザのアプリケーションが認証対象ユーザのアプリケーションにパスワード入力要求信号伝送
ST-24
No
認証対象ユーザの認証完了？
B
Yes
ST-25
ユーザのアプリケーションに認証完了信号伝送
ST-26
ユーザのアプリケーションがデータ格納ユーザのアプリケーションにデータ要求信号伝送
ST-27
No
データ受信完了？
C
ST-28
データ復旧
エンド

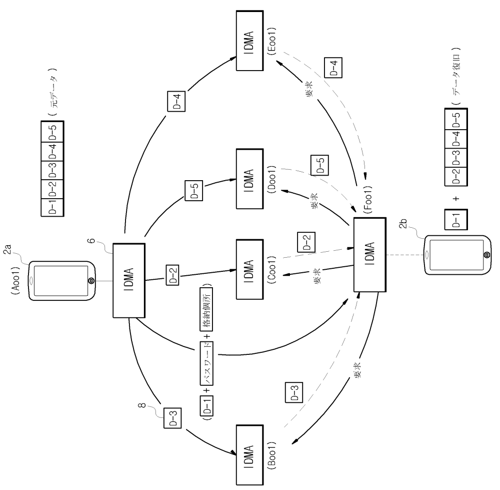
【図１０】


B
ST-30
認証失敗？
Yes
No
ST-31
サーバに認証失敗
情報伝送
ST-32
No
設定時間の経過時
まで無反応？
Yes
ST-33
サーバーに新規な認証
ユーザの情報要求
D

【図１１】


C
ST-40
No
一定時間の経過時
まで特定 の分割データ
未受信？
Yes
ST-41
サーバーに未受信情報伝送
（分割データ情報＋バックアップ先の情報）
ST-42
サーバが分割データ情報のバックアップ先
アプリケーションに分割デー タ伝送
ST-43
バックアップ先アプリケーションが
サーバーに分割データ伝送
ST-44
サーバが分割データをユーザの
アプリケーションに伝送
ST-45
データの復旧
エンド

【図１２】


IDMA
(Aoo1)
(Boo1)
(Coo1)
(Doo1)
(Eoo1)
(Foo1)
2a
2b
6
8
D-1 D-2 D-3 D-4 D-5
D-1
D-2
D-3
D-4
D-5
要求

フロントページの続き

(72)発明者　ナム、ギ　ウォン
大韓民国、０６１５９　ソウル　カンナムーグ、テヘランーロ、４２３、＃１３０２（サムソンードン、ヒョンデ　タワー）
(72)発明者　パク、ギル　ジュ
大韓民国、３４０２２　テジョン　ユソンーグ、ペウル　１ーロ、３５、＃４０８－２００１（クァンピョンードン、テドック　テクノ　バレー４ダンジ　アパート）

審査官　大桃　由紀雄

(56)参考文献　特開２００９－１３９９９０（ＪＰ，Ａ）
特開２００４－１４７２１８（ＪＰ，Ａ）
特開２０１０－１９８３４９（ＪＰ，Ａ）
特開２０１１－２３２８３４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２