(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6371184号
(P6371184)

(45)発行日　平成30年8月8日(2018.8.8)　(24)登録日　平成30年7月20日(2018.7.20)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
H04L 9/14	(2006.01)	H04L	9/00	641
G06F 21/62	(2013.01)	G06F	21/62	

請求項の数 18　(全 25 頁)

(21)出願番号　特願2014-199202(P2014-199202)
(22)出願日　平成26年9月29日(2014.9.29)
(65)公開番号　特開2016-72769(P2016-72769A)
(43)公開日　平成28年5月9日(2016.5.9)
審査請求日　平成29年3月1日(2017.3.1)

(73)特許権者　000233055
株式会社日立ソリューションズ
東京都品川区東品川四丁目１２番７号
(74)代理人　100091096
弁理士　平木　祐輔
(74)代理人　100102576
弁理士　渡辺　敏章
(74)代理人　100101063
弁理士　松丸　秀和
(72)発明者　穂積　真之介
東京都品川区東品川四丁目１２番７号　株式会社日立ソリューションズ内
(72)発明者　青柳　誠
東京都品川区東品川四丁目１２番７号　株式会社日立ソリューションズ内
最終頁に続く

(54)【発明の名称】データ管理システム、データ管理方法、及びクライアント端末

(57)【特許請求の範囲】
【請求項１】
ユーザ認証を行う管理サーバと、少なくとも１つのクライアント端末と、ファイルを格納するクラウドストレージと、を有するデータ管理システムであって、
前記クライアント端末は、
前記クライアント端末の位置情報を前記管理サーバに送信し、
前記位置情報に応じた暗号鍵を取得してファイルを暗号化又は暗号化ファイルを復号化し、
前記管理サーバは、
セキュリティレベルに応じた複数の暗号鍵と、前記クライアント端末の位置に応じてセキュリティレベルを決定するためのポリシと、を管理し、
前記クライアント端末から受信した前記位置情報と前記ポリシとに基づいて、前記クライアント端末のセキュリティレベルを決定し、当該決定されたセキュリティレベルに対応する暗号鍵を前記クライアント端末に送信し、
前記クライアント端末は、前記位置情報に基づく前記セキュリティレベルに対応した前記暗号鍵を取得した後に当該クライアント端末の位置情報に変化を検知した場合、当該変化の後の位置情報に基づく前記セキュリティレベルに対応する暗号鍵を特定し、以前のセキュリティレベルが今回のセキュリティレベルより高い場合には以前取得した前記暗号鍵の少なくとも１つを削除し、以前のセキュリティレベルが今回のセキュリティレベルより低い場合には前記管理サーバから不足する暗号鍵を取得する、

ことを特徴とするデータ管理システム。
【請求項２】
請求項１において、
前記位置情報は、前記クライアント端末のＩＰアドレスの情報と前記クライアント端末の物理的位置の情報を含むことを特徴とするデータ管理システム。
【請求項３】
請求項１において、
前記管理サーバは、特定のネットワーク上及び特定の物理的位置でのみ閲覧が可能とされるデータファイルを暗号化及び復号化するための暗号鍵である極秘鍵と、許可されたネットワーク上でのみ閲覧が可能とされるデータファイルを暗号化及び復号化するための暗号鍵である社外秘鍵と、任意のネットワーク上及び任意の物理的な位置で閲覧が可能とされるデータファイルを暗号化及び復号化する暗号鍵である一般鍵と、を管理することを特徴とするデータ管理システム。
【請求項４】
請求項３において、
前記管理サーバは、（ｉ）前記クライアント端末が前記特定のネットワーク上で動作し、及び特定の物理的な位置にあるときには、前記極秘鍵、前記社外秘鍵、及び前記一般鍵の全てを前記クライアント端末に送信し、（ｉｉ）前記クライアント端末が前記許可されたネットワーク上で動作しているときには、前記社外秘鍵及び前記一般鍵のみを前記クライアント端末に送信し、（ｉｉｉ）前記クライアント端末が前記任意のネットワーク上で動作し、及び前記任意の物理的な位置にあるときには、前記一般鍵のみ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管理システム。
【請求項５】
請求項４において、
前記クライアント端末が前記許可されたネットワーク上で動作しているときに前記極秘鍵でのみ復号可能なデータファイルをダウンロードした場合、前記クライアント端末は、前記許可されたネットワークから前記特定のネットワーク、及び特定の物理的な位置に移動した場合に、前記極秘鍵を前記管理サーバから取得し、当該取得した極秘鍵を用いて前記ダウンロードしたデータファイルを自動的に復号することを特徴とするデータ管理システム。
【請求項６】
ユーザ認証を行う管理サーバと、少なくとも１つのクライアント端末と、ファイルを格納するクラウドストレージと、の間におけるデータ管理方法であって、
前記管理サーバは、セキュリティレベルに応じた複数の暗号鍵と、前記クライアント端末の位置に応じてセキュリティレベルを決定するためのポリシと、を管理しており、
前記クライアント端末が、前記クライアント端末の位置情報を前記管理サーバに送信するステップと、
前記管理サーバが、前記クライアント端末から受信した前記位置情報と前記ポリシとに基づいて、前記クライアント端末のセキュリティレベルを決定し、当該決定されたセキュリティレベルに対応する暗号鍵を前記クライアント端末に送信するステップと、
前記クライアント端末が、前記管理サーバから前記位置情報に応じた暗号鍵を受信し、ファイルを暗号化又は暗号化ファイルを復号化するステップと、
前記クライアント端末が、前記位置情報に基づく前記セキュリティレベルに対応した前記暗号鍵を取得した後に当該クライアント端末の位置情報に変化を検知した場合、当該変化の後の位置情報に基づく前記セキュリティレベルに対応する暗号鍵を特定するステップと、
前記クライアント端末が、以前のセキュリティレベルが今回のセキュリティレベルより高い場合には以前取得した前記暗号鍵の少なくとも１つを削除し、以前のセキュリティレベルが今回のセキュリティレベルより低い場合には前記管理サーバから不足する暗号鍵を取得するステップと、

を有することを特徴とするデータ管理方法。
【請求項７】
請求項６において、
前記位置情報は、前記クライアント端末のＩＰアドレスの情報と前記クライアント端末の物理的位置の情報を含むことを特徴とするデータ管理方法。
【請求項８】
請求項６において、
前記管理サーバは、特定のネットワーク上及び特定の物理的位置でのみ閲覧が可能とされるデータファイルを暗号化及び復号化するための暗号鍵である極秘鍵と、許可されたネットワーク上でのみ閲覧が可能とされるデータファイルを暗号化及び復号化するための暗号鍵である社外秘鍵と、任意のネットワーク上及び任意の物理的な位置で閲覧が可能とされるデータファイルを暗号化及び復号化する暗号鍵である一般鍵と、を管理することを特徴とするデータ管理方法。
【請求項９】
請求項８において、
前記管理サーバは、（ｉ）前記クライアント端末が前記特定のネットワーク上で動作し、及び特定の物理的な位置にあるときには、前記極秘鍵、前記社外秘鍵、及び前記一般鍵の全てを前記クライアント端末に送信し、（ｉｉ）前記クライアント端末が前記許可されたネットワーク上で動作しているときには、前記社外秘鍵及び前記一般鍵のみを前記クライアント端末に送信し、（ｉｉｉ）前記クライアント端末が前記任意のネットワーク上で動作し、及び前記任意の物理的な位置にあるときには、前記一般鍵のみ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管理方法。
【請求項１０】
請求項９において、
さらに、前記クライアント端末が、前記許可されたネットワーク上で動作しているときに前記極秘鍵でのみ復号可能なデータファイルをダウンロードした場合、前記許可されたネットワークから前記特定のネットワーク、及び特定の物理的な位置に移動した場合に、前記極秘鍵を前記管理サーバから取得し、当該取得した極秘鍵を用いて前記ダウンロードしたデータファイルを自動的に復号するステップを有することを特徴とするデータ管理方法。
【請求項１１】
ユーザ認証を行う管理サーバ及びファイルを格納するクラウドストレージと通信するクライアント端末であって、
各種プログラムを格納するメモリと、
前記メモリから各種プログラムを読み込んで実行するプロセッサと、を有し、
前記プロセッサは、
前記クライアント端末の位置情報を前記管理サーバに送信し、
前記管理サーバから、セキュリティレベルに応じた複数の暗号鍵と、前記クライアント端末の位置に応じてセキュリティレベルを決定するためのポリシと、を受信し、
前記位置情報に応じた暗号鍵に基づいてファイルを暗号化又は暗号化ファイルを復号し、
前記位置情報に基づく前記セキュリティレベルに対応した前記暗号鍵を取得した後に当該クライアント端末の位置情報に変化を検知した場合、当該変化の後の位置情報に基づく前記セキュリティレベルに対応する暗号鍵を特定し、以前のセキュリティレベルが今回のセキュリティレベルより高い場合には以前取得した前記暗号鍵の少なくとも１つを削除し、以前のセキュリティレベルが今回のセキュリティレベルより低い場合には前記管理サーバから不足する暗号鍵を取得することを特徴とするクライアント端末。
【請求項１２】
請求項１１において、
前記位置情報は、前記クライアント端末のＩＰアドレスの情報と前記クライアント端末

の物理的位置の情報を含むことを特徴とするクライアント端末。
【請求項１３】
請求項１１において、
前記プロセッサは、前記管理サーバから、特定のネットワーク上及び特定の物理的位置でのみ閲覧が可能とされるデータファイルを暗号化及び復号化するための暗号鍵である極秘鍵と、許可されたネットワーク上でのみ閲覧が可能とされるデータファイルを暗号化及び復号化するための暗号鍵である社外秘鍵と、任意のネットワーク上及び任意の物理的な位置で閲覧が可能とされるデータファイルを暗号化及び復号化する暗号鍵である一般鍵と、を受信することを特徴とするクライアント端末。
【請求項１４】
請求項１３において、
前記プロセッサは、前記管理サーバから、（ｉ）前記クライアント端末が前記特定のネットワーク上で動作し、及び特定の物理的な位置にあるときには、前記極秘鍵、前記社外秘鍵、及び前記一般鍵の全てを受信し、（ｉｉ）前記クライアント端末が前記許可されたネットワーク上で動作しているときには、前記社外秘鍵及び前記一般鍵のみを受信し、（ｉｉｉ）前記クライアント端末が前記任意のネットワーク上で動作し、及び前記任意の物理的な位置にあるときには、前記一般鍵のみを受信することを特徴とするクライアント端末。
【請求項１５】
請求項１４において、
前記プロセッサは、前記クライアント端末が前記許可されたネットワーク上で動作しているときに前記極秘鍵でのみ復号可能なデータファイルをダウンロードした場合、前記許可されたネットワークから前記特定のネットワーク、及び特定の物理的な位置に移動した場合に、前記極秘鍵を前記管理サーバから取得し、当該取得した極秘鍵を用いて前記ダウンロードしたデータファイルを自動的に復号することを特徴とするクライアント端末。
【請求項１６】
請求項１において、
前記クライアント端末は、前記位置情報に基づく前記セキュリティレベルに対応した前記暗号鍵を取得した後に当該クライアント端末の位置情報に変化を検知した場合、当該変化の後の位置情報に基づく前記セキュリティレベルに対応する暗号鍵を特定し、以前のセキュリティレベルが今回のセキュリティレベルより高い場合には以前取得した前記暗号鍵によって複合したファイルを削除することを特徴とするデータ管理システム。
【請求項１７】
請求項６において、
前記クライアント端末が、以前のセキュリティレベルが今回のセキュリティレベルより高い場合には以前取得した前記暗号鍵によって複合したファイルを削除するステップをさらに有するデータ管理方法。
【請求項１８】
請求項１１において、
前記プロセッサは、
前記位置情報に基づく前記セキュリティレベルに対応した前記暗号鍵を取得した後に当該クライアント端末の位置情報に変化を検知した場合、当該変化の後の位置情報に基づく前記セキュリティレベルに対応する暗号鍵を特定し、以前のセキュリティレベルが今回のセキュリティレベルより高い場合には以前取得した前記暗号鍵によって複合したファイルを削除することを特徴とするクライアント端末。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ管理システム、データ管理方法、及びクライアント端末に関し、例えば、ファイルの暗号化・復号に使用する暗号鍵の管理に関するものである。
【背景技術】

【０００２】
近年、コンシューマ向けに提供されていたパブリッククラウドストレージサービスを業務利用することの検討が始まっている。パブリッククラウドストレージサービスが提供するファイル共有機能は、クラウドストレージを利用するメリットの１つとなっている。
【０００３】
しかしながら、パブリッククラウドストレージを業務利用する際にセキュリティ面の不安を抱くユーザが多く、現状は個人での利用用途に留まっている。そのためセキュリティ対策の１つとして、クラウドストレージに格納するファイルを暗号化して運用する方式が考えられている。これに関連して、クラウドストレージに格納するファイルを暗号化することに対応したソフトウェア製品が販売されているが、パブリッククラウドストレージサービスのファイル共有機能と暗号化を両立させている製品は少ない。
【０００４】
例えば、特許文献１には、ファイルをクラウドストレージにアップロードする際に、鍵管理サーバから取得した暗号鍵で暗号化を行い、ファイルをクラウドストレージからダウンロードする際、暗号化ファイルに埋め込まれた識別情報から共有の種類を識別し、鍵管理サーバから取得した暗号鍵の中の適切な鍵で復号を行うシステムが記載されている。
【０００５】
また、特許文献２には、移動通信端末に保存された情報がネットワーク経由で漏洩することを防止するために、移動通信端末の物理的な位置情報およびネットワーク上の位置情報に応じて通信制御ポリシを自端末に適用するネットワークシステムが記載されている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２０１４－１２７７２１号公報
【特許文献２】特開２０１３－３８７１６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
しかしながら、特許文献１に記載されているシステムでは、クラウドストレージおよび鍵管理サーバへのアクセスはネットワーク上の任意の場所から可能であるため、システムユーザの故意または過失により機密情報の漏洩に繋がる可能性がある。
【０００８】
また、特許文献２に記載されているシステムでは、端末の位置によっては認証サーバのみしかアクセスできないため、機密情報の漏洩は防止できるものの、システムユーザの利便性が著しく制限されていて好ましくない。
【０００９】
本発明はこのような状況に鑑みてなされたものであり、ユーザの利便性をも考慮しつつ、情報漏洩のリスクを低減し、クラウドストレージ利用におけるセキュリティを確保するための技術を提供するものである。
【課題を解決するための手段】
【００１０】
上記課題を解決するために、本発明では、クライアント端末は、クライアント端末の位置情報を管理サーバに送信し、位置情報に応じた暗号鍵を取得してファイルを暗号化又は暗号化ファイルを復号する処理を実行する。一方、管理サーバは、セキュリティレベルに応じた複数の暗号鍵と、クライアント端末の位置に応じてセキュリティレベルを決定するためのポリシと、を管理する、また、管理サーバは、クラインアント端末から受信した位置情報と前記ポリシとに基づいて、クライアント端末のセキュリティレベルを決定し、当該決定されたセキュリティレベルに対応する暗号鍵を前記クライアント端末に送信する処理を実行する。
【００１１】

本発明に関連する更なる特徴は、本明細書の記述、添付図面から明らかになるものである。また、本発明の態様は、要素及び多様な要素の組み合わせ及び以降の詳細な記述と添付される特許請求の範囲の様態により達成され実現される。

【００１２】

本明細書の記述は典型的な例示に過ぎず、本発明の特許請求の範囲又は適用例を如何なる意味においても限定するものではないことを理解する必要がある。

【発明の効果】

【００１３】

本発明によれば、情報漏洩のリスクを低減し、クラウドストレージ利用におけるセキュリティを確保することができる。また、ユーザの利便性に対する犠牲も少なくて済む。

【図面の簡単な説明】

【００１４】

【図１】本発明の実施形態によるデータ管理システム１０００の概略構成を示す図である。

【図２】本発明の実施形態による管理サーバ１００の詳細な機能構成を示すブロック図である。

【図３】本発明の実施形態によるクライアント端末２００の詳細な機能構成を示すブロック図である。

【図４】本発明の実施形態による、データベース１７０に格納されているポリシ１７３の構成例を示す図である。

【図５】本発明の実施形態による、管理サーバ１００のユーザ認証処理の概要を説明するための図である。図５Ａは、新たなユーザを登録する処理、図５Ｂは、登録後のユーザを認証する処理を示している。

【図６】本発明の実施形態による、クライアント端末２００がデータファイル５１２を暗号化してクラウドストレージ３００に格納（アップロード）する処理の概要を説明するための図である。

【図７】本発明の実施形態による、クライアント端末２００がデータファイル５１２をクラウドストレージ３００から取得（ダウンロード）して復号化する処理の概要を説明するための図である。

【図８】本発明の実施形態による、クライアント端末２００のＯＳ（オペレーティングシステム）上におけるファイルシステムの構成を示す図である。

【図９】クライアント端末２００が暗号化フォルダ６３０内に格納された新たなデータファイルをクラウドストレージ３００に送信（アップロード）する処理を説明するためのフローチャートである。

【図１０】クライアント端末２００がクラウドストレージ３００から暗号化データファイルをダウンロードする処理の詳細を説明するためのフローチャートである。

【図１１】本発明の実施形態による、位置情報の変化に応じて暗号鍵を削除或いは取得する処理の詳細を説明するためのフローチャートである。

【図１２】図４に示されるポリシで運用した場合の具体例を説明するためのシーケンス図である。

【発明を実施するための形態】

【００１５】

以下、添付図面を参照して本発明の実施形態について説明する。添付図面では、機能的に同じ要素は同じ番号で表示される場合もある。なお、添付図面は本発明の原理に則った具体的な実施形態と実装例を示しているが、これらは本発明の理解のためのものであり、決して本発明を限定的に解釈するために用いられるものではない。

【００１６】

本実施形態では、当業者が本発明を実施するのに十分詳細にその説明がなされているが、他の実装・形態も可能で、本発明の技術的思想の範囲と精神を逸脱することなく構成・構造の変更や多様な要素の置き換えが可能であることを理解する必要がある。従って、以

降の記述をこれに限定して解釈してはならない。

【００１７】

更に、本発明の実施形態は、後述されるように、汎用コンピュータ上で稼動するソフトウェアで実装しても良いし専用ハードウェア又はソフトウェアとハードウェアの組み合わせで実装しても良い。

【００１８】

なお、以後の説明では「テーブル」形式によって本発明の各情報について説明するが、これら情報は必ずしもテーブルによるデータ構造で表現されていなくても良く、リスト、ＤＢ、キュー等のデータ構造やそれ以外で表現されていても良い。そのため、データ構造に依存しないことを示すために「テーブル」、「リスト」、「ＤＢ」、「キュー」等について単に「情報」と呼ぶことがある。

【００１９】

また、各情報の内容を説明する際に、「識別情報」、「識別子」、「名」、「名前」、「ＩＤ」という表現を用いることが可能であり、これらについてはお互いに置換が可能である。

【００２０】

以下では「各機能部（例えば、ユーザ認証部）」を主語（動作主体）として本発明の実施形態における各処理について説明を行うが、各機能部はプログラムで構成され、プログラムはプロセッサによって実行されることで定められた処理をメモリ及び通信ポート（通信制御装置）を用いながら行うため、プロセッサを主語とした説明としてもよい。また、プログラムを主語として開示された処理は認証サーバ等の計算機、情報処理装置が行う処理としてもよい。プログラムの一部または全ては専用ハードウェアで実現してもよく、また、モジュール化されていても良い。各種プログラムはプログラム配布サーバや記憶メディアによって各計算機にインストールされてもよい。

【００２１】

＜データ管理システムの構成＞

図１は、本発明の実施形態によるデータ管理システム１０００の概略構成を示す図である。データ管理システム１０００は、管理サーバ（認証サーバと称することも可能）１００と、クライアント端末２００と、クラウドストレージ３００と、を有し、これらは、例えばインターネットなどのネットワーク３０１を介して接続されている。

【００２２】

管理サーバ１００は、クライアント端末２００を利用するユーザのユーザＩＤを管理する認証サーバとして動作する。また、後述の図２で説明するように、管理サーバ１００は、クライアント端末２００がデータファイルを暗号化および復号する際に使用する暗号鍵を管理する。

【００２３】

クライアント端末２００は、管理サーバ１００から取得した暗号鍵を用いてデータファイルを暗号化し、暗号化後のデータファイルをクラウドストレージ３００に格納する。また、クライアント端末２００は、管理サーバ１００から取得した暗号鍵を用いて、クラウドストレージ３００から取得した暗号化データファイルを復号化する。クライアント端末２００が管理サーバ１００から暗号鍵を取得する際には、管理サーバ１００による認証を受ける必要がある。説明を簡易化するため、クラウドストレージ３００にアクセスする際には必ずしも認証は必要でないものとするが、認証処理を設けてもよい。クライアント端末２００は、例えば、パーソナルコンピュータやモバイル端末などのコンピュータである。以下では総称してクライアント端末２００とする。

【００２４】

クラウドストレージ３００は、クライアント端末２００が暗号化したデータファイルを格納する。クラウドストレージ３００は、ネットワーク３０１に接続された記憶装置によって構成されており、ネットワーク３０１を介してデータを読み書きすることができる。クラウドストレージ３００を提供している事業者は、管理サーバ１００（およびその構成

要素）やクライアント端末２００が所属する事業者とは必ずしも同じでなくても良い。
【００２５】
＜管理サーバの構成＞
図２は、本発明の実施形態による管理サーバ１００の詳細な機能構成を示すブロック図である。管理サーバ１００は、クライアント端末２００がデータファイルを暗号化する際に使用する暗号鍵を、ユーザ毎の認証を用いて暗号化した上で管理し、クライアント端末２００からのリクエストに応じてその暗号鍵を暗号化したままで送信する。
【００２６】
管理サーバ１００は、各種プログラムを実行する演算部であるＣＰＵ（プロセッサ）１０１と、各種プログラムを格納するメモリ１０２と、指示を入力したり、演算結果を出力したりする入出力デバイス（入力デバイスとして、キーボード、マウス、マイク等、出力デバイスとしてディスプレイ、プリンタ、スピーカ等）１０３と、クライアント端末２００やクラウドストレージ３００と通信するための通信デバイス１０４と、各種データを格納するデータベース１７０と、を有している。
【００２７】
メモリ１０２は、プログラムとして、極秘鍵暗号化部１１０と、社外秘鍵暗号化部１２０と、一般鍵暗号化部１３０と、ＰＷ鍵暗号化部１４０と、暗号鍵送信部１５０と、ポリシ管理部１６０と、データベース１７０と、を有している。暗号鍵送信部１５０は、さらに、プログラムとして、認証部１５１と、送信部１５２と、を有している。また、ポリシ管理部１６０は、プログラムとして、ポリシ送受信部１６１と、ポリシ検索部１６２と、ポリシ設定部１６３と、を有している。データベース１７０以外の機能部については、後述の図３以降で改めて説明する。
【００２８】
データベース１７０は、クライアント端末２００がデータファイルを暗号化する際に使用する暗号鍵を管理するデータベースである。この暗号鍵は３種類存在する。極秘鍵１７１２は、クライアント端末２００が社内にある場合にのみ取得できる暗号鍵である。社外秘鍵１７１４は、クライアント端末２００が許可されたネットワーク上にある場合にのみ取得できる暗号鍵である。一般鍵１７１６は、任意のネットワーク上から取得できる暗号鍵である。
【００２９】
データベース１７０は、ユーザ毎の認証情報を用いて上記３種類の鍵を暗号化し、ユーザ毎に設けたユーザテーブル１７１内の各レコードとして格納する。ここでは説明を簡易化するため、管理サーバ１００はパスワードによって各ユーザを認証するものと仮定し、そのパスワードを暗号鍵（以下ではＰＷ鍵１７１８と呼ぶ）として上記３種類の暗号鍵を暗号化するものとする。レコード１７１１、１７１３、１７１５は、それぞれ極秘鍵１７１２、社外秘鍵１７１４、一般鍵１７１６をＰＷ鍵１７１８によって暗号化したデータである。
【００３０】
ユーザテーブル１７１はさらに、ユーザ毎のＰＷ鍵１７１８を、システム管理者のみが管理する管理鍵１７２によって暗号化し、レコード１７１７として格納する。管理鍵１７２は、ユーザテーブル１７１とは別の記憶領域に保持する。例えばセッション管理領域に格納することができる。ＰＷ鍵１７１８を複製して管理することにより、ユーザがパスワードを忘れた場合であっても、管理者が管理鍵１７２を用いてＰＷ鍵１７１８を復号した上で、これを用いて極秘鍵１７１２、社外秘鍵１７１４、一般鍵１７１６をそれぞれ復号し、新たなパスワードを発行してそのパスワードにより各暗号鍵を再暗号化することができる。すなわち、図２に示すように暗号鍵を２重に暗号化している場合であっても、認証情報を再発行することができる。
【００３１】
データベース１７０は、ハードディスク装置などの記憶装置を用いて構成することができる。その他の機能部は、図２に示されるように、これらの機能を実装したプログラムを

ＣＰＵ（Central Processing Unit）などの演算装置が実行することによって実現するようにしているが、これらの機能を実現する回路デバイスなどのハードウェアを用いて構成することもできる。プログラムによって実現する場合、これら機能部は、コンピュータ読取可能な記憶媒体（例えば、メモリ、ハードディスク、ＳＳＤ（Solid State Drive）等の記録装置、ＩＣカード、ＳＤカード、ＤＶＤ等の記録媒体）に格納することができる。

【００３２】

＜クライアント端末の構成＞

図３は、本発明の実施形態によるクライアント端末２００の詳細な機能構成を示すブロック図である。

【００３３】

クライアント端末２００は、各種プログラムを実行する演算部であるＣＰＵ（プロセッサ）２０１と、各種プログラムを格納するメモリ２０２と、各種データを格納する記憶装置２５０と、指示を入力したり、演算結果を出力したりする入出力デバイス（入力デバイスとして、キーボード、マウス、マイク等、出力デバイスとしてディスプレイ、プリンタ、スピーカ等）２０３と、管理サーバ１００と通信するための通信デバイス２０４と、を有している。

【００３４】

メモリ２０２は、プログラムとしての、端末位置情報変化検知部２１０と、端末位置情報通知部２２０と、ポリシ取得部２３０と、ネットワーク接続部２４０と、を有している。記憶装置２５０以外の各部は、ハードウェアとして構成されても良いし、ソフトウェア上の機能として実現しても良い。

【００３５】

端末位置情報変化検知部２１０は、クライアント端末２００の位置変化を検知するための処理を実行するデバイス又はプログラムである。本明細書において、この「位置」は、クライアント端末２００のネットワーク上の位置や物理的な位置、又はこれらの組み合わせを意味するものとする。例えばネットワーク接続部２４０に割り当てられたＩＰアドレスによるネットワーク上の位置、クライアント端末２００が備えるＧＰＳ装置により検出されたクライアント端末２００の地球における物理的な位置、クライアント端末２００が接続している無線ＬＡＮのアクセスポイントのＳＳＩＤ（Service Set ID）、ＭＡＣアドレス等の情報に基づいたネットワーク的及び物理的な位置、又はこれらの位置の組み合わせ等が相当する。

【００３６】

端末位置情報変化検知部２１０は、記憶装置２５０に格納される端末位置変化閾値情報２５１を参照し、自端末の位置の変化（ＩＰアドレスによるネットワーク上の位置、及びＧＰＳによる物理的位置）を検知する。すなわち、端末位置情報変化検知部２１０は、ＩＰアドレスによるネットワーク上の位置及び物理的位置を端末位置変化閾値情報２５１と比較し、いずれかの位置が端末位置変化閾値情報２５１に記載されている条件を満たさなくなった場合に、位置が変化したと検知する。端末位置変化閾値情報２５１については後述する。

【００３７】

端末位置情報通知部２２０は、端末位置情報変化検知部２１０によって検知された端末位置情報を通知する処理を実行するデバイス又はプログラムである。端末位置の変化が検出される度に管理サーバ１００に当該端末位置情報が通知される。

【００３８】

ポリシ取得部２３０は、管理サーバ１００のポリシ送受信部１６１（図２）からポリシ情報２５４を取得する処理を実行するデバイス又はプログラムである。

【００３９】

ネットワーク接続部２４０は、クライアント端末２００とネットワーク３０１とを接続する装置であり、例えば有線ＬＡＮ（Local Area Network）装置や無線ＬＡＮ装置、３Ｇ（第３世代移動通信システム）無線装置、４Ｇ（第４世代移動通信システム）無線装置な

どが相当する。
【００４０】
記憶装置２５０は、本実施形態に係る通信制御の実現に必要とされる情報の記憶に使用される。例えば、端末位置変化閾値情報２５１、端末識別情報２５２、認証サーバアドレス情報２５３、ポリシ情報２５４が記憶される。なお、記憶装置２５０には、不図示の任意の情報が格納されていてもよい。
【００４１】
端末位置変化閾値情報２５１は、端末位置情報変化検知部２１０がクライアント端末２００（自端末）の位置に変化が発生したか否かを判断するために使用する情報である。端末位置変化閾値情報２５１には、例えば（１）企業の建屋が含まれる緯度・経度の範囲、（２）社内ネットワークにおいてクライアント端末２００のネットワーク接続部２４０に割り当てられるＩＰアドレスの範囲、（３）その両方などが記憶される。
【００４２】
例えば、端末位置変化閾値情報２５１に、企業等ユーザが所属する組織の建屋が含まれる緯度・経度の範囲が記憶されている場合、クライアント端末２００が備えるＧＰＳの観測値が記憶されている所定の緯度・経度の範囲を外れたとき、端末位置情報変化検知部２１０は、クライアント端末２００（自端末）の社内から社外への移動を検知する。
【００４３】
端末識別情報２５２は、クライアント端末２００を一意に特定する情報であり、例えば、クライアント端末２００の端末固有番号、ユーザ名とパスワードの組、クライアント端末２００のネットワーク接続部２４０のＭＡＣアドレス、これら情報の組み合わせ等が相当する。
【００４４】
認証サーバアドレス情報２５３は、管理サーバ１００のＩＰアドレス又はドメイン名で与えられる。
【００４５】
ポリシ情報２５４の詳細は後述するが、クライアント端末２００の通信制御に適用される条件が相当する。
【００４６】
＜ポリシの構成例＞
図４は、本発明の実施形態による、データベース１７０に格納されているポリシ１７３の構成例を示す図である。当該ポリシ１７３は、ユーザ毎に設定しても良いが、ここではシステムで共通な情報として設定されているものとする。
【００４７】
ポリシ１７３は、ポリシ名４０１と、ネットワーク的位置範囲４０２と、物理的位置範囲４０３と、機密度４０４と、を構成情報として含んでいる。図４は、例として３つのポリシ情報４０５～４０７を示している。クライアント端末２００は、管理サーバ１００にログインする度、或いはクライアント端末２００の位置に変化を検知する度に、最新のポリシ１７３を取得し、ポリシ情報２５４に格納する。
【００４８】
ポリシ情報４０５は、ネットワーク接続部２４０に割り当てられたＩＰアドレスがネットワーク的位置範囲４０２「１９２．１６８．０．０／２４」に含まれ、かつ、クライアント端末２００のＧＰＳによる物理的な位置が物理的位置範囲４０３「建屋が含まれる緯度・経度の範囲」に含まれる場合に、そのネットワークを「社内ネットワーク」と認識して、機密度が「極秘/社外秘/一般」である暗号鍵の取得を許可することを示している。
【００４９】
ポリシ情報４０５が当てはまる状況としては、例えば社内において、クライアント端末２００が利用されており、クライアント端末２００が社内のＷｉ－Ｆｉアクセスポイントに接続している場合が挙げられる。
【００５０】

ポリシ情報４０６は、ネットワーク接続部２４０に割り当てられたＩＰアドレスがネットワーク的位置範囲４０２「１０．０．０．０／２４」に含まれ、かつ、クライアント端末２００のＧＰＳによる物理的な位置が任意の場所にある場合に、そのネットワークを「許可ネットワーク」と認識して、機密度が「社外秘/一般」である暗号鍵の取得を許可することを示している。

【００５１】

ポリシ情報４０６が当てはまる状況としては、例えばクライアント端末２００が社外で利用されているが、あらかじめ許可されたネットワークに接続している場合が挙げられる。

【００５２】

ポリシ情報４０７は、ネットワーク接続部２４０に割り当てられたＩＰアドレスによるネットワーク上の位置及びＧＰＳによる物理的な位置に関わらず、そのネットワークを「社外ネットワーク」と認識して、機密度が「一般」である暗号鍵の取得を許可することを示している。

【００５３】

ポリシ情報４０７が当てはまる状況としては、社内ネットワークおよび社内ネットワークに当てはまらない任意のネットワークに接続している場合が挙げられる。

【００５４】

＜ユーザ認証処理の概要＞

図５は、本発明の実施形態による、管理サーバ１００のユーザ認証処理の概要を説明するための図である。図５Ａは、新たなユーザを登録する処理、図５Ｂは、登録後のユーザを認証する処理を示している。以下ではｕｓｅｒ＿Ａに関する処理を例として各処理を説明する。

【００５５】

クライアント端末２００のユーザであるｕｓｅｒ＿Ａは、管理サーバ１００にアクセスし、ｕｓｅｒ＿Ａを新規ユーザとして登録するよう依頼する。以下では管理サーバ１００がパスワードを自動的に発行するものと仮定する。

【００５６】

認証部１５１は、クライアント端末２００から新規ユーザであるｕｓｅｒ＿Ａを登録するよう要求するリクエストを受け取ると、ｕｓｅｒ＿Ａに対応するパスワードｕｓｅｒ＿Ａ＿ＰＷを発行し、その対応関係を保持する。以後ｕｓｅｒ＿Ａは、パスワードｕｓｅｒ＿Ａ＿ＰＷを用いて管理サーバ１００にログインすることができる。新規ユーザを登録する処理は自動化してもよいし、管理者が介在してそのユーザを新規登録してもよいか否かを判断した後に登録するようにしてもよい。

【００５７】

認証部１５１は、ｕｓｅｒ＿Ａの極秘鍵１７１２を例えば乱数によって生成する。同様に社外秘鍵１７１４、一般鍵１７１６を生成する。管理鍵１７２はあらかじめ適当な手法によって生成しておく。

【００５８】

極秘鍵暗号化部１１０は、パスワードｕｓｅｒ＿Ａ＿ＰＷまたはこれから一意に導出した値をＰＷ鍵１７１８として極秘鍵１７１２を暗号化し、レコード１７１１としてユーザテーブル１７１に格納する。ｕｓｅｒ＿Ａとレコード１７１１の対応関係は、例えばｕｓｅｒ＿Ａのユーザ ＩＤをレコード１７１１と対応付けることによって定義してもよいし、ユーザ毎にユーザテーブル１７１を作成することによって定義してもよい。

【００５９】

社外秘鍵暗号化部１２０、一般鍵暗号化部１３０も同様に、ＰＷ鍵１７１８を用いてそれぞれ社外秘鍵１７１４と一般鍵１７１６を暗号化し、それぞれレコード１７１３、１７１５として格納する。ＰＷ鍵暗号化部１４０は、ＰＷ鍵１７１８を複製して管理鍵１７２によって暗号化し、レコード１７１７として格納する。

【００６０】

クライアント端末２００のユーザがデータファイルを暗号化または復号化するときは、まず管理サーバ１００にログインして各暗号鍵を取得する必要がある。ユーザはクライアント端末２００を介して管理サーバ１００にユーザＩＤｕｓｅｒ＿Ａ、パスワードｕｓｅｒ＿Ａ＿ＰＷおよび端末位置情報通知部２２０から通知されたネットワーク上の位置情報を送信する。認証部１５１はそのユーザＩＤ、パスワードおよびネットワーク上の位置情報を用いて認証処理を実施する。認証許可する場合は、送信部１５２がそのユーザおよびネットワーク上の位置情報に対応する鍵として、極秘鍵１７１２、社外秘鍵１７１４、一般鍵１７１６の中からポリシで取得を許可された鍵をデータベース１７０から読み出し、クライアント端末２００に送信する。ただしこれらの鍵は、ＰＷ鍵１７１８によって暗号化されたままである。

【００６１】

端末位置情報変化検知部２１０によって位置情報の変化を検知した場合は、クライアント端末２００は、ポリシ情報２５４の内容に応じて暗号鍵の取得および削除を行う。例えば、図４の社内ネットワーク４０５に該当する位置から許可ネットワーク４０６に該当する位置にクライアント端末２００が移動した場合は、取得済みの暗号鍵のうち極秘鍵１７１２を削除する。反対に許可ネットワーク４０６に該当する位置から社内ネットワーク４０５に該当する位置にクライアント端末２００が移動した場合は、極秘鍵を取得する。この場合、内部で保存しているユーザＩＤｕｓｅｒ＿Ａ、パスワードｕｓｅｒ＿Ａ＿ＰＷを使用して自動的に認証処理を行ってもよいし、ユーザに再度認証処理を行わせてもよい。

【００６２】

＜ファイルアップロード処理の概要＞

図６は、本発明の実施形態による、クライアント端末２００がデータファイル５１２を暗号化してクラウドストレージ３００に格納（アップロード）する処理の概要を説明するための図である。ここでは社内でのみ閲覧可能としたいデータファイル５１２を使用する場合を想定する。

【００６３】

ユーザは、データファイル５１２をクラウドストレージ３００に格納する前に、予め図５で説明したように管理サーバ１００にログインして、ポリシ１７３で取得が許可されている暗号鍵を取得しておく。クライアント端末２００は、パスワードｕｓｅｒ＿Ａ＿ＰＷを用いて管理サーバ１００から取得した各レコードを復号し、暗号鍵を取得する。データファイル５１２は、社内でのみ閲覧が可能なため、ユーザは、データファイル５１２を暗号化するための暗号鍵として極秘鍵１７１２を選択する。クライアント端末２００は、極秘鍵１７１２を用いてデータファイル５１２を暗号化し、暗号化データファイル５１１を作成する。クライアント端末２００は、暗号化データファイル５１１をクラウドストレージ３００に格納（送信）する。

【００６４】

同様に、データファイル５１２を許可されたネットワーク上で閲覧可能としたい場合は、ユーザは、データファイル５１２を暗号化するための暗号鍵として社外秘鍵１７１４を選択する。データファイル５１２を任意のネットワーク上で閲覧可能としたい場合は、ユーザは、データファイル５１２を暗号化するための暗号鍵として一般鍵１７１６を選択する。クライアント端末２００は、選択された暗号鍵を用いてデータファイル５１２を暗号化し、クラウドストレージ３００に格納する。

【００６５】

クライアント端末２００は、データファイル５１２を暗号化する際に、上記３種類の暗号鍵のうちいずれの種類のものを用いたかを示す情報を、暗号化データファイル５１１内に埋め込む。ただし、暗号鍵の種類が分かれば足りるため、個々の暗号鍵そのものを個別に特定する情報を埋め込む必要はない。

【００６６】

＜ファイルダウンロード処理の概要＞

図７は、本発明の実施形態による、クライアント端末２００がデータファイル５１２を

クラウドストレージ３００から取得（ダウンロード）して復号化する処理の概要を説明するための図である。ここでは図６と同様に、社内でのみ閲覧可能としたいデータファイル５１２を使用する場合を想定する。

【００６７】

ユーザは、データファイル５１２をクラウドストレージ３００から取得する前に、図６と同様にあらかじめポリシ１７３で取得が許可されている暗号鍵を管理サーバ１００から取得する。クライアント端末２００は各暗号鍵を復号する。

【００６８】

ユーザは、クライアント端末２００を介してクラウドストレージ３００にアクセスし、暗号化データファイル５１１を取得する。暗号化データファイル５１１内には、同ファイルが極秘鍵を用いて暗号化されている旨を示す情報が埋め込まれている。したがって、クライアント端末２００は、ｕｓｅｒ＿Ａの極秘鍵１７１２を用いて暗号化データファイル５１１を復号するよう試みる。暗号化データファイル５１１がｕｓｅｒ＿Ａの極秘鍵１７１２によって暗号化されている場合は、暗号化データファイル５１１を復号化することができる。

【００６９】

同様に、データファイル５１２が社外秘鍵１７１４で暗号化されたファイルである場合は、クライアント端末２００は、社外秘鍵１７１４を用いて暗号化データファイル５１１を復号化する。データファイル５１２が一般鍵１７１６で暗号化されたファイルである場合は、クライアント端末２００は、一般鍵１７１６を用いて暗号化データファイル５１１を復号化する。

【００７０】

＜ファイルシステムの構成＞

図８は、本発明の実施形態による、クライアント端末２００のＯＳ（オペレーティングシステム）上におけるファイルシステムの構成を示す図である。クライアント端末２００は、図６～図７で説明したように個々のデータファイル５１２を暗号化または復号化することができるが、ユーザがその都度暗号鍵を選択するなどの作業が発生するため、ユーザにとって負担が生じる。そこで、クライアント端末２００は、ファイルシステム上の所定フォルダ以下に格納したデータファイルを一括して暗号化または復号化し、さらにはクラウドストレージ３００との間でファイルを同期化することができる。図８は、そのフォルダ構成例を説明するものである。クライアント端末２００のファイルシステムは、暗号化ファイルを格納する同期フォルダ６２０と、暗号化処理される平文ファイルを格納する暗号化フォルダ６３０を有する。

【００７１】

（ｉ）同期フォルダ６２０は、クライアント端末２００がクラウドストレージ３００に送信し、またはクライアント端末２００がクラウドストレージ３００から取得したデータファイル（暗号化されたファイル）を格納するフォルダである。クライアント端末２００は、同期フォルダ６２０を常時監視しており、同期フォルダ６２０内に新たなデータファイルが格納されると、そのデータファイルをクラウドストレージ３００に送信する。また、クライアント端末２００は、必要に応じて定期的にクラウドストレージ３００に接続し、新たな暗号化データファイルが存在する場合はダウンロードして同期フォルダ６２０内に格納する。

【００７２】

同期フォルダ６２０内には、サブフォルダを設けることができる。同期フォルダ６２０内のフォルダ／ファイル構成とクラウドストレージ３００上のフォルダ／ファイル構成は同期させることが望ましい。

【００７３】

クライアント端末２００が複数のクラウドストレージ３００を利用する場合は、同期フォルダ６２０内に、各クラウドストレージ３００に対応するサブフォルダを設け、クラウドストレージ３００毎に同期処理を実施することができる。図８に示すサブフォルダ６２

１と６２２は、２つのクラウドストレージ３００（ＣｌｏｕｄＳｔｏｒａｇｅＡ、ＣｌｏｕｄＳｔｏｒａｇｅＢ）に対応する。

【００７４】

（ii）暗号化フォルダ６３０は、クライアント端末２００がクラウドストレージ３００に送信する前に暗号化すべきデータファイル（平文ファイル）を格納し、またはクラウドストレージ３００から取得した暗号化データファイルを復号したデータファイルを格納するフォルダである。クライアント端末２００は、暗号化フォルダ６３０を常時監視しており、暗号化フォルダ６３０内に新たなデータファイルが格納されると、そのデータファイルを暗号化して同期フォルダ６２０に格納する。同期フォルダ６２０に格納されたデータファイルは、上述のようにクラウドストレージ３００へ送信される。またクライアント端末２００は、同期フォルダ６２０内に新たな暗号化データファイルが格納されると、その暗号化データファイルを復号化して暗号化フォルダ６３０に格納する。

【００７５】

（iii）クライアント端末２００は、暗号化フォルダ６３０内のフォルダ／ファイル構成を、同期フォルダ６２０内のファイル／フォルダ構成と同期させる。したがって、同期フォルダ６２０内に複数のクラウドストレージ３００毎のサブフォルダが存在する場合は、暗号化フォルダ６３０内にも同じフォルダ構成を作成する。サブフォルダ６３１と６３２は、それぞれサブフォルダ６２１と６２２に対応する。ただしファイルの拡張子については、暗号化されているか否かを区別するため適当に変更することができる。図８においては、暗号化されているデータファイルには元の「ファイル名＋拡張子」に加えて拡張子「．ｃｒｙｐｔｏ」を付与した例を示した。

【００７６】

（iv）次に、使用する暗号鍵を区別する手法について説明する。ファイルを暗号化する鍵は、ユーザによって暗号化フォルダ６３０毎に設定するものとする。例えば、社外秘鍵１７１４に対応するフォルダに置かれたデータファイルについては社外秘鍵１７１４を用いて暗号化する。図８においては、サブフォルダ６３２内のフォルダ「Ｉｎｔｅｒｎａｌ」がこれに相当する。一般鍵１７１６に対応したフォルダに置かれたデータファイルについては一般鍵１７１６を用いて暗号化する。図８には示していないが、一般鍵１７１６に対応するフォルダを設けることができる。これらに当てはまらないデータファイルについては極秘鍵１７１２を用いて暗号化する。

【００７７】

クライアント端末２００がクラウドストレージ３００から新たな暗号化データファイルを取得した際には、図７において説明したように、いずれの種類の暗号鍵を用いるべきかを示す情報が暗号化データファイル内に埋め込まれているので、その情報に対応する暗号鍵を用いて暗号化データファイルを復号することができる。あるいはデータファイルを暗号化する場合と同様に、例えば社外秘鍵１７１４で暗号化したデータファイルを格納するフォルダ内のデータファイルについては社外秘鍵１７１４を用いて復号化してもよい。

【００７８】

暗号化データファイル内に埋め込まれている情報とフォルダの間の対応関係が矛盾する場合は、どのように処理すべきかを別途設定ファイルなどに定義しておき、その設定にしたがって処理すればよい。例えば、極秘鍵１７１２で暗号化したデータファイルを格納するフォルダ内に、社外秘鍵１７１４を用いて暗号化されている旨の情報が埋め込まれている暗号化データファイルが格納されている場合は、極秘鍵１７１２と社外鍵１７１４を双方用いて復号化を試行し、復号に成功した方を採用することができる。あるいはその暗号化データファイルについては復号化せずそのまま暗号化フォルダ６３０内に格納することもできる。この処理は、後述するステップＳ９０５～Ｓ９１０において適用することができる。

【００７９】

（v）ファイルをクラウドストレージ３００にアップロードする場合、ユーザが暗号化フォルダ６３０に対象ファイルを格納すると、その対象ファイルは暗号化され、同期フォル

ダ６２０内に格納されるとともに、クラウドストレージ３００に送信され、格納される。
【００８０】
ファイルをクラウドストレージ３００からダウンロードする場合、暗号化データファイルがクラウドストレージ３００からクライアント端末に送信され、同期フォルダ６３０に格納される。例えば、ユーザが社内から社外に移動している場合には、復号に使える鍵の数は減っている（社外から社内に移動した場合には復号に使える鍵の数は増える）。従って、極秘鍵で復号すべきファイルに関しては、社外で暗号化データファイルを取得するのみで復号されない。その後、ユーザが社内に戻ってから当該暗号化データファイルが自動的に復号されて平文となったファイルが暗号化フォルダ６３０に格納されるようにしても良い。
【００８１】
＜ファイルアップロード処理の詳細＞
図９は、クライアント端末２００が暗号化フォルダ６３０内に格納された新たなデータファイルをクラウドストレージ３００に送信（アップロード）する処理を説明するためのフローチャートである。以下、図９の各ステップについて説明する。
【００８２】
（ｉ）ステップＳ９０１
ユーザが認証情報（ユーザＩＤとパスワード）を入力すると、クライアント端末２００は、当該認証情報をクライアント端末２００のネットワーク上の位置情報と併せて管理サーバ１００に送信する。
【００８３】
（ii）ステップＳ９０２～Ｓ９０３
管理サーバ１００の認証部１５１は、クライアント端末２００から受け取った認証情報を用いてユーザ認証を実施する（Ｓ９０２）。認証拒否する場合はその旨を示す応答をクライアント端末２００に送信し、クライアント端末２００はユーザ認証に失敗した旨を示すダイアログを画面表示して（Ｓ９０３）、本フローチャートは終了する。認証許可する場合、処理はステップＳ９０４へ進む。
【００８４】
（iii）ステップＳ９０４
送信部１５２は、データベース１７０から当該ユーザおよびネットワーク上の位置情報に応じて極秘鍵１７１２、社外秘鍵１７１４、及び一般鍵１７１６を取得し、クライアント端末２００に送信する。ただし、図２で説明したように、これら３つの鍵はＰＷ鍵１７１８によって暗号化されているので、クライアント端末２００は、当該ユーザの認証情報を用いてこれら暗号鍵を復号化する。
【００８５】
（iv）ステップＳ９０５
クライアント端末２００は、同期フォルダ６２０内に格納されているファイル構成と暗号化フォルダ６３０内に格納されているファイル構成を比較し、同期フォルダ６２０内に格納されているファイル構成に追加や更新が発生しているか否かを判定する。追加や更新が発生している場合、処理はステップＳ９０６へ進み、発生していない場合、処理はステップＳ９０７へスキップする。
【００８６】
（v）ステップＳ９０６
クライアント端末２００は、暗号化データファイルに埋め込まれた情報に基づき、対応する暗号鍵を用いてその暗号化データファイルを復号し、暗号化フォルダ６３０にコピーする。同期フォルダ６２０内の暗号化データファイルが削除されていた場合は、暗号化フォルダ６３０内の対応するデータファイルを削除する。
【００８７】
（vi）ステップＳ９０７
クライアント端末２００は、暗号化フォルダ６３０内のファイル構成に追加や更新があ

ったかを定期的に確認する。追加や更新が発生している場合、処理はステップＳ９０８へ進み、発生していない場合、処理はステップＳ９０９へスキップする。

【００８８】

（vii）ステップＳ９０８

クライアント端末２００は、暗号化フォルダ６３０内において追加または更新されたデータファイルを対応する暗号鍵で暗号化し、同期フォルダ６２０にコピーする。クライアント端末２００は、同期フォルダ６２０にコピーされた暗号化データファイルをクラウドストレージ３００にアップロードする。

【００８９】

（viii）ステップＳ９０９～Ｓ９１０

クライアント端末２００は、ユーザがログアウトしたか否かを判定し（Ｓ９０９）、ログアウトした場合は暗号化フォルダ６３０の監視を終了する。ログアウトしていない場合、処理はステップＳ９０５に戻り、同様の処理が繰り返される（Ｓ９１０）。

【００９０】

＜ファイルダウンロード処理の詳細＞

図１０は、クライアント端末２００がクラウドストレージ３００から暗号化データファイルをダウンロードする処理の詳細を説明するためのフローチャートである。ステップＳ１００１～Ｓ１００４は図９のステップＳ９０１～Ｓ９０４と同様であるため、以下ではステップＳ１００５以降のみについて説明する。

【００９１】

（i）ステップＳ１００５

クライアント端末２００は、クラウドストレージ３００からダウンロードした暗号化データファイルを、同期フォルダ６２０に格納する。クライアント端末２００は、クラウドストレージ３００からダウンロードした暗号化データファイルに埋め込まれた識別情報を確認することにより、復号化処理において使用すべき暗号鍵を特定する。

【００９２】

（ii）ステップＳ１００６～Ｓ１０１０

クライアント端末２００は、ステップＳ１００５における判定結果に基づき、対応する暗号鍵を用いて暗号化データファイルを復号化する。復号化によって得られたデータファイルは、暗号化フォルダ６３０内の対応するフォルダに格納される。

【００９３】

＜位置情報に応じた暗号鍵の削除／取得処理の詳細＞

（１）処理内容

図１１は、本発明の実施形態による、位置情報の変化に応じて暗号鍵を削除或いは取得する処理の詳細を説明するためのフローチャートである 。

【００９４】

（i）ステップＳ１１０１

端末位置情報変化検知部２１０がクライアント端末２００の位置の変化を検知すると、端末位置情報通知部２２０は、位置変化後のクライアント端末２００の位置情報（ＩＰアドレス及び物理的位置の情報）を管理サーバ１００に送信する。管理サーバ１００は、最新のポリシ１７３を当該クライアント端末２００に送信する。

【００９５】

（ii）ステップＳ１１０２

ポリシ取得部２３０は、管理サーバ１００から送信されてきた最新のポリシ１７３が取得できた場合には、当該ポリシを最新のポリシ情報２５４として保持する。

【００９６】

（iii）ステップＳ１１０３

端末位置情報変化検知部２１０は、最新のポリシ１７３を取得することに成功したか判断する。成功した場合（ステップＳ１１０３でＹｅｓの場合）、処理はステップＳ１１０４に移行する。失敗した場合（ステップＳ１１０３でＮｏの場合）、処理はステップＳ１

１０５に移行する。
【００９７】
（iv）ステップＳ１１０４
端末位置情報変化検知部２１０は、最新のポリシ（ポリシ情報２５４）を参照する。
【００９８】
（v）ステップＳ１１０５
端末位置情報変化検知部２１０は、以前に取得済のポリシ（ポリシ情報２５４）を参照する。
【００９９】
（vi）ステップＳ１１０６
端末位置情報変化検知部２１０は、ポリシ情報２５４を参照し、クライアント端末２００の現在の位置情報と当該ポリシ情報２５４とを照合することにより、取得可能な暗号鍵の機密度の情報を取得する。例えば、社内ネットワーク４０５から許可ネットワーク４０６にクライアント端末２００が移動した場合には、社外秘鍵及び一般鍵のみが使える状態となる。
【０１００】
（vii）ステップＳ１１０７
端末位置情報変化検知部２１０は、現在のポリシに基づくと取得不可とされる鍵を保持しているか否か判断する。取得不可とされる鍵を保持している場合（ステップＳ１１０７でＹｅｓの場合）、処理はステップＳ１１０８に移行する。保持していない場合（ステップＳ１１０７でＮｏの場合）、処理はステップＳ１１０９に移行する。例えば、（vi）の例で言えば、許可ネットワークで取得不可とされる「極秘鍵」を有しているため、処理はステップＳ１１０８に移行することになる。
【０１０１】
（viii）ステップＳ１１０８
端末位置情報変化検知部２１０は、クライアント端末２００の現在の位置（ポリシ名４０１）では取得不可とされる鍵を削除する。つまり、上記例では、「極秘鍵」を削除することになる。
【０１０２】
（ix）ステップＳ１１０９
端末位置情報変化検知部２１０は、クライアント端末２００の現在の位置（ポリシ名４０１）で使用可能であるが保持していない鍵があるか判断する。使用可能であるが保持していない鍵がある場合（ステップＳ１１０９でＹｅｓの場合）、処理はステップＳ１１１０に移行する。例えば、許可ネットワーク４０６から社内ネットワーク４０５にクライアント端末２００が移動した場合には、極秘鍵が使えるにも拘らず保持していない鍵となる。当該鍵を既に持っている場合（ステップＳ１１０９でＮｏの場合）、本フローチャートは終了する。
【０１０３】
（x）ステップＳ１１１０
端末位置情報変化検知部２１０は、管理サーバ１００から取得可能な鍵を取得する。
【０１０４】
（２）具体例
図１２は、図４に示されるポリシで運用した場合の具体例を説明するためのシーケンス図である 。
【０１０５】
（i）シーケンス１
クライアント端末２００が社内ネットワークに位置しているときに、ユーザの操作により管理サーバ１００に対して認証を行ったとする。このときクライアント端末２００は、１つも暗号鍵を保持していないものとする。
【０１０６】

（ii）シーケンス２
認証が完了すると、クライアント端末２００のポリシ取得部２３０は、管理サーバ１００から最新のポリシ１７３を取得し、ポリシ情報２５４として保持する。この時点ではまだ暗号鍵は取得されていない。
【０１０７】
（iii）シーケンス３
クライアント端末２００の端末位置情報変化検知部２１０は、クライアント端末２００の現在の位置情報からポリシ（ポリシ名４０１）を社内ネットワーク４０５であると判定し、管理サーバ１００から社内ネットワークの機密度４０４に対応する極秘鍵、社外秘鍵、及び一般鍵を取得する。ここで、初めて暗号鍵が取得されることとなる。
【０１０８】
（iv）シーケンス４
クライアント端末２００を保持するユーザが物理的位置を移動したり、ＩＰアドレスを変更したりして社内ネットワークから社外ネットワークに移動したものとする。単にネットワークを移動しただけでは、保持している暗号鍵に変化はなく、この時点で保持している暗号鍵は、極秘鍵、社外秘鍵、及び一般鍵である。
【０１０９】
（v）シーケンス５
端末位置情報変化検知部２１０は、社外ネットワークに移動したため、ポリシ情報２５４を参照して、取得済の暗号鍵（極秘鍵、社外秘鍵、及び一般鍵）のうち、極秘鍵及び社外秘鍵を削除する。従って、この時点でクライアント端末２００は、一般鍵のみ保持していることとなる。
【０１１０】
（vi）シーケンス６
続いて、ユーザがＩＰアドレスを変更して社外ネットワークから許可ネットワークに移動したものとする。ネットワークを移動したこの時点では、クライアント端末２００はまだ一般鍵のみ保持している状態である。
【０１１１】
（vii）シーケンス７
端末位置情報変化検知部２１０は、許可ネットワークに移動したためポリシ情報２５４を参照して、管理サーバ１００から未取得の暗号鍵（極秘鍵及び社外秘鍵）のうち社外秘鍵を取得する。従って、この時点でクライアント端末２００は、社外秘鍵及び一般鍵を保持していることとなる。
【０１１２】
以上のように、本発明の実施形態によるクライアント端末２００では、当該クライアント端末２００の位置（ＩＰアドレス、及び物理的位置）の変化により暗号鍵を取得したり、削除したりして、使うことのできる鍵を制限している。
【０１１３】
＜まとめ＞
（i）本発明では、ファイルを暗号化する暗号鍵に機密度を設定することを可能とする。例えば、個人で利用するファイルを暗号化する鍵は従来１つで十分だったが、「極秘」「社外秘」「一般」等の機密度が設定された暗号鍵から選択可能とする。また、ＰＣやモバイル端末の物理的な位置情報およびネットワーク上の位置情報を利用して、取得できる暗号鍵のコントロールを可能とする。例えば、社内ネットワークから鍵管理サーバにログインを行った場合はすべての暗号鍵を取得できるが、ポリシで許可されたネットワークからログインを行った場合は「社外秘」「一般」の機密度が設定された暗号鍵のみ取得可能、その他のネットワークからログインを行った場合は「一般」の機密度が設定された暗号鍵のみ取得可能とする。さらに、ネットワーク上の位置情報が変化した場合に暗号鍵の制御を行う。例えば、社内ネットワークからポリシで許可されたネットワークに切り替わった場合は、「極秘」の暗号鍵および「極秘」の暗号鍵で復号したファイルを削除する。これ

により、社外で極秘のファイルを参照すること、および極秘のファイルを復号する暗号鍵が社外に流出することを防止し、クラウドストレージ上のデータファイルのセキュリティを向上させる。つまり、本発明によれば、情報の機密度に応じてファイルを暗号化および復号できる物理的な位置およびネットワーク上の位置をコントロールすることができる。また、ポリシで暗号鍵の取得が許可されている物理的な位置およびネットワーク上の位置の外に暗号鍵が流出することを防止できる。

【０１１４】

（ii）本発明は、上記した実施形態に限定されるものではなく、様々な変形例が含まれる。上記実施形態は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施形態の構成の一部を他の実施形態の構成に置き換えることもできる。また、ある実施形態の構成に他の実施形態の構成を加えることもできる。また、各実施形態の構成の一部について、他の構成を追加・削除・置換することもできる。

【０１１５】

例えば、上記実施形態においては、暗号鍵と復号鍵が同一である暗号方式を前提としたが、暗号鍵と復号鍵が異なる場合（例えば公開鍵暗号方式）においても適用することができる。この場合は、管理サーバ１００が暗号鍵と復号鍵のペアをそれぞれ管理しておき、クライアント端末２００は暗号鍵と復号鍵のいずれを必要とするかを管理サーバ１００へ通知するようにすればよい。

【０１１６】

また、極秘鍵１７１２、社外秘鍵１７１４、一般鍵１７１６を、特許文献１に記載されているサービス共有やシステム共有と組み合わせて、さらに細かいポリシを適用することもできる。

【０１１７】

また、本明細書ではクラウドストレージの利用を前提としたが、暗号ファイルの格納先としてファイルサーバやプライベートクラウドストレージを利用することもできる。

【０１１８】

さらに、上記実施形態においては、ユーザを認証するための認証情報としてパスワードを例示したが、クライアント端末２００が各暗号鍵を復号することができれば、その他の認証情報を用いることもできる。

【０１１９】

また、上記実施形態においては、フォルダ構成としてＷｉｎｄｏｗｓ（登録商標）を想定したが、その他のＯＳ上においても同様の仕組みを提供することができる。

【０１２０】

（iii）本発明は、実施形態の機能を実現するソフトウェアのプログラムコードによっても実現できる。この場合、プログラムコードを記録した記憶媒体をシステム或は装置に提供し、そのシステム或は装置のコンピュータ（又はＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出す。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコード自体、及びそれを記憶した記憶媒体は本発明を構成することになる。このようなプログラムコードを供給するための記憶媒体としては、例えば、フレキシブルディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどが用いられる。

【０１２１】

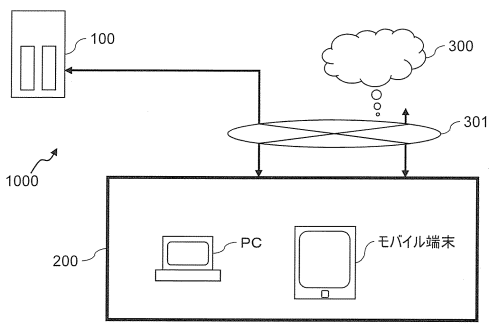
また、プログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）などが実際の処理の一部又は全部を行い、その処理によって前述した実施の形態の機能が実現されるようにしてもよい。さらに、記憶媒体から読み出されたプログラムコードが、コンピュータ上のメモリに書きこまれた後、そのプログラムコードの指示に基づき、コンピュータのＣＰＵなどが実際の処理の一部又は全部を行い、その処理によって前述した実施の形態の機能が実現されるようにしてもよい。

【０１２２】
さらに、実施の形態の機能を実現するソフトウェアのプログラムコードを、ネットワークを介して配信することにより、それをシステム又は装置のハードディスクやメモリ等の記憶手段又はＣＤ－ＲＷ、ＣＤ－Ｒ等の記憶媒体に格納し、使用時にそのシステム又は装置のコンピュータ（又はＣＰＵやＭＰＵ）が当該記憶手段や当該記憶媒体に格納されたプログラムコードを読み出して実行するようにしても良い。
【０１２３】
最後に、ここで述べたプロセス及び技術は本質的に如何なる特定の装置に関連することはなく、コンポーネントの如何なる相応しい組み合わせによってでも実装できることを理解する必要がある。更に、汎用目的の多様なタイプのデバイスがここで記述した教授に従って使用可能である。ここで述べた方法のステップを実行するのに、専用の装置を構築するのが有益であることが判るかもしれない。また、実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。本発明は、具体例に関連して記述したが、これらは、すべての観点に於いて限定の為ではなく説明の為である。本分野にスキルのある者には、本発明を実施するのに相応しいハードウェア、ソフトウェア、及びファームウエアの多数の組み合わせがあることが解るであろう。例えば、記述したソフトウェアは、アセンブラ、Ｃ／Ｃ＋＋、ｐｅｒｌ、Ｓｈｅｌｌ、ＰＨＰ、Ｊａｖａ（登録商標）等の広範囲のプログラム又はスクリプト言語で実装できる。
【０１２４】
さらに、上述の実施形態において、制御線や情報線は説明上必要と考えられるものを示しており、製品上必ずしも全ての制御線や情報線を示しているとは限らない。全ての構成が相互に接続されていても良い。
【符号の説明】
【０１２５】
１００・・・管理サーバ
１０１・・・ＣＰＵ
１０２・・・メモリ
１０３・・・入出力デバイス
１０４・・・通信デバイス
１１０・・・極秘鍵暗号化部
１２０・・・社外秘鍵暗号化部
１３０・・・一般鍵暗号化部
１４０・・・ＰＷ鍵暗号化部
１５０・・・暗号鍵送信部
１６０・・・ポリシ管理部
１７０・・・データベース
１７２・・・管理鍵
１７３・・・ポリシ
２００・・・クライアント端末
２０１・・・ＣＰＵ
２０２・・・メモリ
２０３・・・入出力デバイス
２０４・・・通信デバイス
２１０・・・端末位置情報変化検知部
２２０・・・端末位置情報通知部
２３０・・・ポリシ取得部
２４０・・・ネットワーク接続部
２５０・・・記憶装置

３００・・・クラウドストレージ
３０１・・・ネットワーク

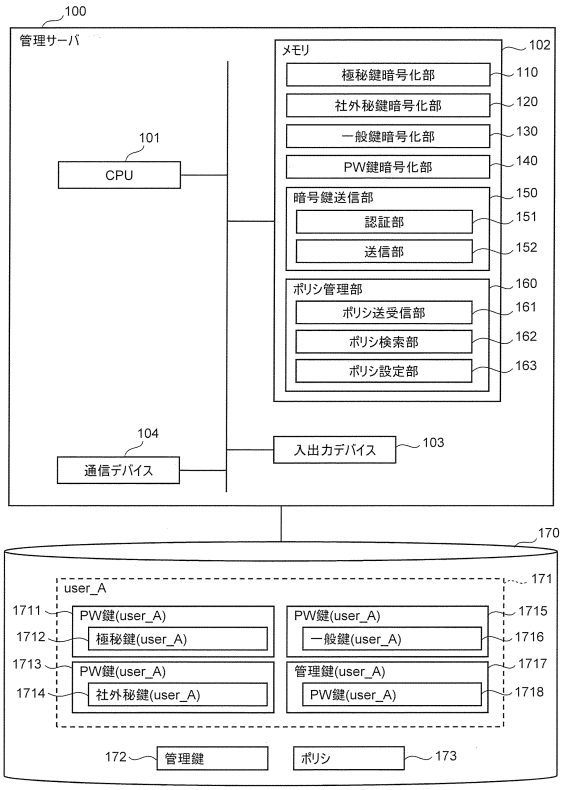
【図１】

図１



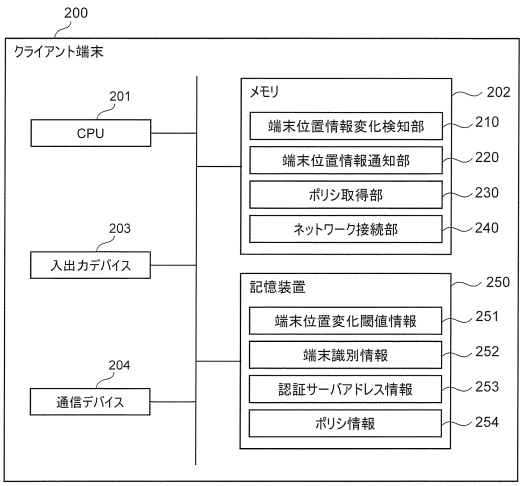
【図２】

図２



【図３】

図３



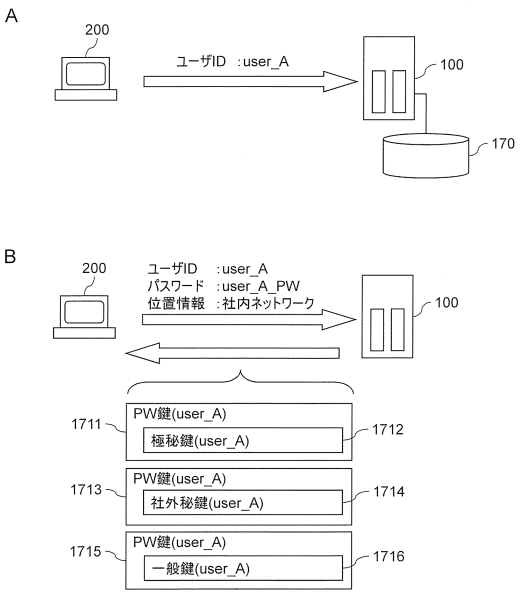
【図４】

図４

	401 ポリシ名	402 ネットワーク的位置範囲	403 物理的位置範囲	404 機密度
405	社内ネットワーク	192.168.0.0/24	建屋が含まれる緯度・経度の範囲	極秘/社外秘/一般
406	許可ネットワーク	10.0.0.0/24	任意	社外秘/一般
407	社外ネットワーク	任意	任意	一般

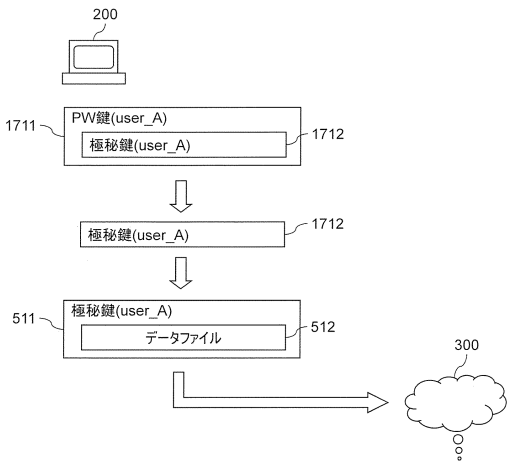
【図５】

図５



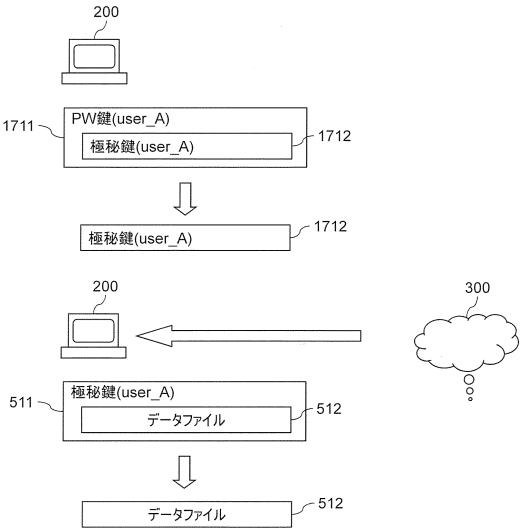
【図６】

図６



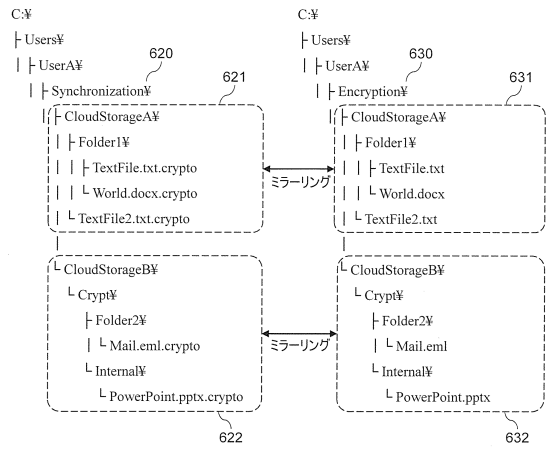
【図７】

図７



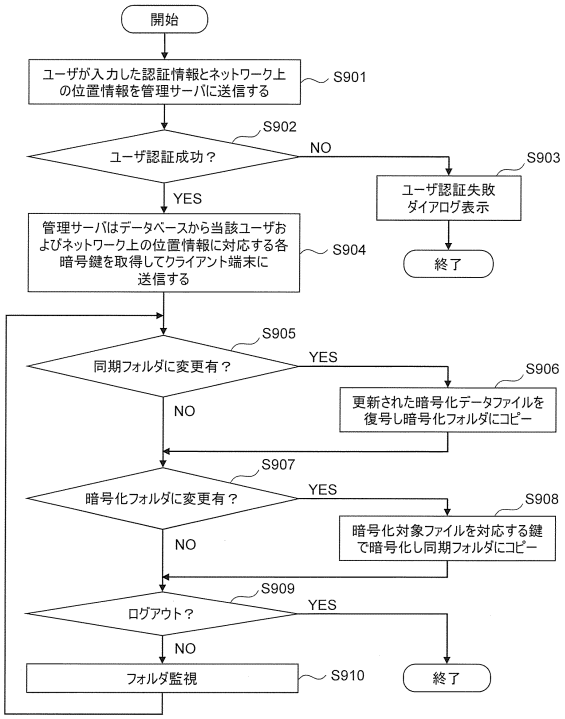
【図８】

図８



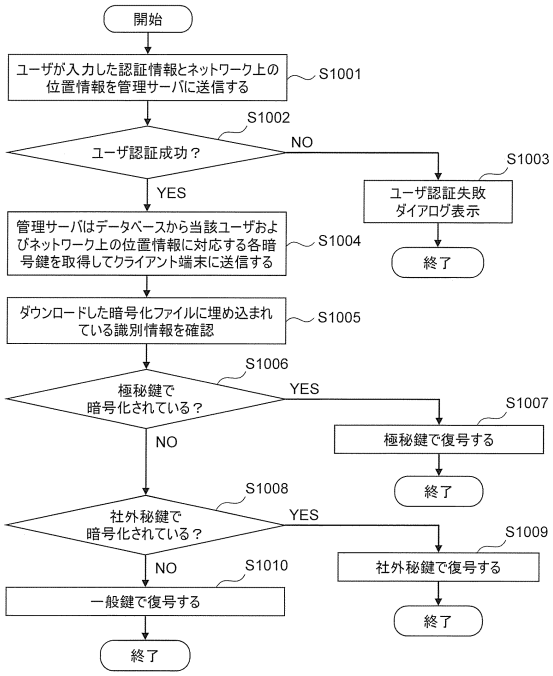
【図９】

図９



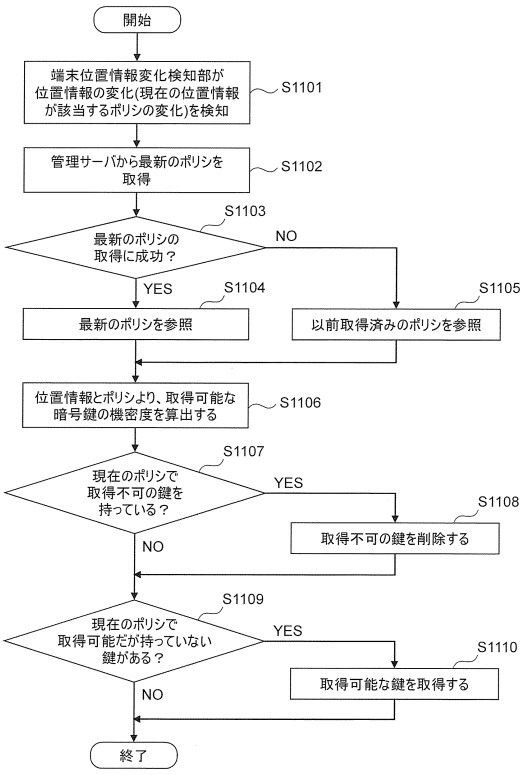
【図１０】

図１０



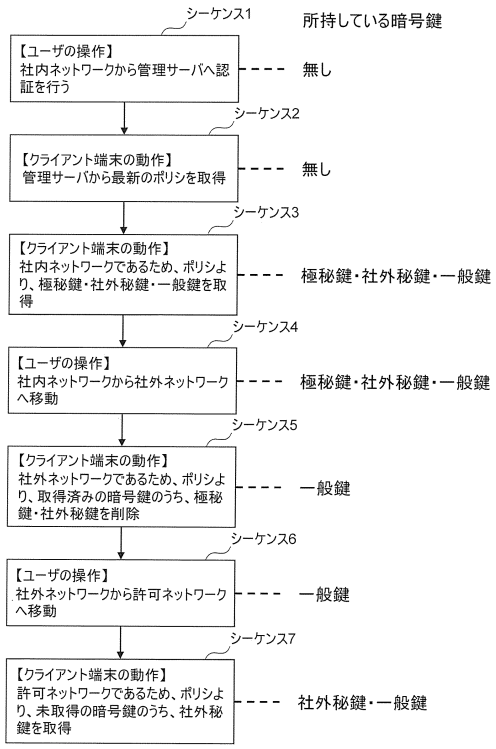
【図１１】

図１１



【図１２】

図１２


シーケンス1
所持している暗号鍵
【ユーザの操作】
社内ネットワークから管理サーバへ認証を行う
無し
シーケンス2
【クライアント端末の動作】
管理サーバから最新のポリシを取得
無し
シーケンス3
【クライアント端末の動作】
社内ネットワークであるため、ポリシより、極秘鍵・社外秘鍵・一般鍵を取得
極秘鍵・社外秘鍵・一般鍵
シーケンス4
【ユーザの操作】
社内ネットワークから社外ネットワークへ移動
極秘鍵・社外秘鍵・一般鍵
シーケンス5
【クライアント端末の動作】
社外ネットワークであるため、ポリシより、取得済みの暗号鍵のうち、極秘鍵・社外秘鍵を削除
一般鍵
シーケンス6
【ユーザの操作】
社外ネットワークから許可ネットワークへ移動
一般鍵
シーケンス7
【クライアント端末の動作】
許可ネットワークであるため、ポリシより、未取得の暗号鍵のうち、社外秘鍵を取得
社外秘鍵・一般鍵

フロントページの続き

審査官　青木　重徳

(56)参考文献　特開２００８－０１５６６９（ＪＰ，Ａ）
特開平０５－２４４１５０（ＪＰ，Ａ）
特開２００７－０９４５４８（ＪＰ，Ａ）
特開２００６－３３３１６４（ＪＰ，Ａ）
米国特許出願公開第２００８／０３０７０２０（ＵＳ，Ａ１）
クラウドストレージに必要な情報漏洩対策　秘文　Ｃｌｏｕｄ　Ｄａｔａ　Ｐｒｏｔｅｃｔｉｏｎ（秘文ＣＰ），日立イノベーションフォーラム２０１３，日本，株式会社日立ソリューションズ，２０１３年１０月３０日
佐藤　亮太　ほか，スマートフォンにおける利用環境に応じた機能制御機構の実装と評価，電子情報通信学会技術研究報告，日本，一般社団法人電子情報通信学会，２０１３年　2月２８日，Ｖｏｌ．１１２、Ｎｏ．４６６，ｐｐ．２０３－２０８

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／６２
Ｈ０４Ｌ　　９／１４