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

特許第6182589号
(P6182589)

(45)発行日　平成29年8月16日(2017.8.16)　(24)登録日　平成29年7月28日(2017.7.28)

(51)Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F	21/62	318
G06F 12/00	(2006.01)	G06F	12/00	537H
G06F 21/60	(2013.01)	G06F	21/60	320
H04L 9/08	(2006.01)	H04L	9/00	601C
		H04L	9/00	601E

請求項の数 12　(全 26 頁)

(21)出願番号　特願2015-503217(P2015-503217)
(86)(22)出願日　平成25年2月28日(2013.2.28)
(65)公表番号　特表2015-517146(P2015-517146A)
(43)公表日　平成27年6月18日(2015.6.18)
(86)国際出願番号　PCT/US2013/028224
(87)国際公開番号　WO2013/148052
(87)国際公開日　平成25年10月3日(2013.10.3)
審査請求日　平成27年9月4日(2015.9.4)
(31)優先権主張番号　13/430,607
(32)優先日　平成24年3月26日(2012.3.26)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　501113353
シマンテック　コーポレーション
Ｓｙｍａｎｔｅｃ　Ｃｏｒｐｏｒａｔｉｏｎ
アメリカ合衆国，カリフォルニア州　９４０４３，マウンテン　ビュー，エリス　ストリート　３５０
(74)代理人　100147485
弁理士　杉村　憲司
(72)発明者　ボゴラド・ウォルター
アメリカ合衆国　カリフォルニア州　９４５２６　ダンビル　グラスゴーサークル　８０５

審査官　脇岡　剛

最終頁に続く

(54)【発明の名称】安全な第三者データ記憶のためのシステム及び方法

(57)【特許請求の範囲】
【請求項１】
安全な第三者データ記憶のためのコンピュータ実装方法であって、該方法の少なくとも一部分が少なくとも１つのプロセッサを備えるサーバ側コンピューティングデバイスによって実施され、前記方法が、
クライアント側キーが前記サーバ側コンピューティングデバイスにて利用不能である間に、前記サーバ側コンピューティングデバイスで、ユーザアカウントの下に暗号化されていないファイルを記憶するクライアントシステムからの第１の要求を受信することと、
前記第１の要求に応答して、前記クライアント側キーが前記サーバ側コンピューティングデバイスにて利用不能である間に、前記サーバ側コンピューティングデバイスで、前記ユーザアカウントに指定された非対称キーペアであって、暗号化キーと、前記クライアント側キーで暗号化されている復号キーとを含む、非対称キーペアを識別することと、
クライアント側キーが前記サーバ側コンピューティングデバイスにて利用不能である間に、前記サーバ側コンピューティングデバイスで、前記暗号化キーを用いて前記暗号化されていないファイルを暗号化することによって前記暗号化されていないファイルから暗号化ファイルを生成することと、
前記サーバ側コンピューティングデバイスで、前記ユーザアカウントの下に前記暗号化ファイルを記憶することと、
前記サーバ側コンピューティングデバイスで、前記ユーザアカウントの下に記憶された前記暗号化ファイルにアクセスする前記クライアントシステムからの第２の要求を識別す

ることであって、前記要求されたアクセスが前記暗号化ファイルの復号を必要とする、要求を識別することと、
前記第２の要求に応答して、前記ユーザアカウントに指定された前記非対称キーペアを識別することと、
前記クライアントシステムから、前記クライアント側キーを受信することと、
前記サーバ側コンピューティングデバイスで、前記復号キーを前記クライアント側キーで復号することと、
前記サーバ側コンピューティングデバイスで、前記復号キーを使用して、前記暗号化ファイルの暗号化されていないバージョンにアクセスすることと、
前記暗号化ファイルの前記暗号化されていないバージョンにアクセスするように指定された追加のユーザアカウントを識別することであって、追加の非対称キーペアが、前記追加のユーザアカウントに指定され、前記追加の非対称キーペアが、追加の暗号化キーと、追加のクライアント側キーで暗号化されている追加の復号キーとを含む、追加のユーザアカウントを識別することと、
前記復号キーを前記追加の暗号化キーで暗号化することと、
前記追加のユーザアカウントを介して前記暗号化ファイルに更にアクセスする追加のクライアントシステムからの追加の要求を識別することであって、前記追加の要求されたアクセスが、前記暗号化ファイルの復号を必要とする、追加の要求を識別することと、
前記復号キーを前記追加の復号キーで復号することと、
前記復号キーを使用して、前記追加のユーザアカウントを介して前記暗号化ファイルの前記暗号化されていないバージョンにアクセスすることと、を含む、コンピュータ実装方法。
【請求項２】
前記復号キーを使用して、前記暗号化ファイルにアクセスすることが、
前記暗号化ファイルを暗号化するために使用されるファイルキーであって、前記暗号化キーで暗号化される、ファイルキーを識別することと、
前記ファイルキーを前記復号キーで復号することと、
前記暗号化ファイルを前記ファイルキーで復号することと、を含む、請求項１に記載のコンピュータ実装方法。
【請求項３】
前記暗号化ファイルの前記暗号化されていないバージョンへのアクセスを前記追加のユーザアカウントに提供することが、
前記暗号化ファイルを暗号化するために使用されるファイルキーであって、前記暗号化キーで暗号化される、ファイルキーを識別することと、
前記ファイルキーを前記復号キーで復号することと、
前記ファイルキーのコピーを前記追加の暗号化キーで暗号化することと、を含む、請求項１に記載のコンピュータ実装方法。
【請求項４】
前記暗号化ファイルにアクセスすることが、前記暗号化ファイルの前記暗号化されていないバージョンを前記クライアントシステムに送信することを含む、請求項１に記載のコンピュータ実装方法。
【請求項５】
前記復号キーを使用して、前記暗号化ファイルの前記暗号化されていないバージョンにアクセスすることが、前記暗号化ファイルの前記暗号化されていないバージョンを記述するメタデータを生成することを含み、前記メタデータを生成することは前記暗号化ファイルの前記暗号化されていないバージョン内のコンテンツに基づいて前記暗号化ファイルの前記暗号化されていないバージョンのプレビューを生成することを含む、請求項１に記載のコンピュータ実装方法。
【請求項６】
前記暗号化ファイルの前記暗号化されていないバージョンを記述する前記メタデータを

生成することが、
前記暗号化ファイルの前記暗号化されていないバージョンにセキュリティ走査を実施することと、
前記暗号化ファイルの前記暗号化されていないバージョン内のコンテンツに基づいて、前記暗号化ファイルの前記暗号化されていないバージョンを索引付けすることとのうちの少なくとも１つを含む、請求項５に記載のコンピュータ実装方法。
【請求項７】
前記暗号化されていないファイルから前記暗号化ファイルを生成することは、
前記暗号化されていないファイルの少なくとも１つの特性に基づいてファイルキーを生成することと、
前記暗号化されていないファイルを前記ファイルキーで暗号化することと、
前記ファイルキーを前記暗号化キーで暗号化することと、を含む、請求項１に記載のコンピュータ実装方法。
【請求項８】
前記暗号化ファイルを前記ファイルキーで暗号化される追加の暗号化ファイルで重複排除することを更に含む、請求項７に記載のコンピュータ実装方法。
【請求項９】
前記クライアント側キーを受信することが、前記クライアント側キーを不揮発性メモリ内に記憶することなく前記クライアント側キーを揮発性メモリ内に記憶することを含む、請求項１に記載のコンピュータ実装方法。
【請求項１０】
前記復号キーを使用して、前記暗号化ファイルの前記暗号化されていないバージョンにアクセスすることが、
前記ユーザアカウントを含む複数のユーザアカウントに指定された第３の非対称キーペアであって、第３の暗号化キーと、前記暗号化キーで暗号化されている第３の復号キーとを含む、第３の非対称キーペアを識別することと、
前記第３の復号キーを前記復号キーで復号することと、
前記暗号化ファイルを暗号化するために使用されるファイルキーであって、前記第３の暗号化キーで暗号化される、ファイルキーを識別することと、
前記ファイルキーを前記第３の復号キーで復号することと、
前記暗号化ファイルを前記ファイルキーで復号することと、を含む、請求項１に記載のコンピュータ実装方法。
【請求項１１】
安全な第三者データ記憶のためのシステムであって、該システムが、
クライアント側キーがサーバ側コンピューティングデバイスにて利用不能である間に、前記サーバ側コンピューティングデバイスで、ユーザアカウントの下に暗号化されていないファイルを記憶するクライアントシステムからの第１の要求を識別するようにプログラムされる識別モジュールと、
前記第１の要求に応答して、前記クライアント側キーが前記サーバ側コンピューティングデバイスにて利用不能である間に、前記サーバ側コンピューティングデバイスで、前記ユーザアカウントに指定された非対称キーペアであって、暗号化キーと、前記クライアント側キーで暗号化されている復号キーとを含む、非対称キーペアを識別するようにプログラムされるキーモジュールと
復号モジュールであって、
前記クライアント側キーが前記サーバ側コンピューティングデバイスにて利用不能である間に、前記サーバ側コンピューティングデバイスで、前記暗号化キーを用いて前記暗号化されていないファイルを暗号化することによって前記暗号化されていないファイルから暗号化ファイルを生成し、
前記サーバ側コンピューティングデバイスで、前記ユーザアカウントの下に前記暗号化ファイルを記憶するようにプログラムされる復号モジュールであって、

前記識別モジュールは、前記サーバ側コンピューティングデバイスで、前記ユーザアカウントの下に記憶された前記暗号化ファイルにアクセスする前記クライアントシステムからの第２の要求を識別するようにさらにプログラムされており、前記要求されたアクセスが前記暗号化ファイルの復号を必要としており、

前記キーモジュールは、前記第２の要求に応答して、前記ユーザアカウントに指定された前記非対称キーペアを識別するようにさらにプログラムされている、

復号モジュールと、

前記クライアントシステムから、前記クライアント側キーを受信するようにプログラムされる受信モジュールであって、

前記復号モジュールは、前記サーバ側コンピューティングデバイスで、前記復号キーを前記クライアント側キーで復号するようにさらにプログラムされている、

受信モジュールと、

前記サーバ側コンピューティングデバイスで、前記復号キーを使用して、前記暗号化ファイルの暗号化されていないバージョンにアクセスするようにプログラムされるアクセスモジュール

とを備えるシステムであって、

前記アクセスモジュールは、

前記暗号化ファイルの前記暗号化されていないバージョンにアクセスするように指定された追加のユーザアカウントを識別するようにさらにプログラムされ、追加の非対称キーペアが、前記追加のユーザアカウントに指定され、前記追加の非対称キーペアが、追加の暗号化キーと、追加のクライアント側キーで暗号化されている追加の復号キーとを含み、

前記復号キーを前記追加の暗号化キーで暗号化するようにさらにプログラムされており、

前記識別モジュールは、前記追加のユーザアカウントを介して前記暗号化ファイルに更にアクセスする追加のクライアントシステムからの追加の要求を識別するようにさらにプログラムされており、前記追加の要求されたアクセスが、前記暗号化ファイルの復号を必要とし、

前記復号モジュールは、前記復号キーを前記追加の復号キーで復号するようにさらにプログラムされており、

前記アクセスモジュールは、前記復号キーを使用して、前記追加のユーザアカウントを介して前記暗号化ファイルの前記暗号化されていないバージョンにアクセスするようにさらにプログラムされており、

前記サーバ側コンピューティングデバイスは、前記識別モジュール、前記キーモジュール、前記受信モジュール、前記復号モジュール、及び前記アクセスモジュールを実行するように構成された少なくとも１つのプロセッサを備える、システム。

【請求項１２】

前記アクセスモジュールが、前記復号キーを使用して、

前記暗号化ファイルを暗号化するために使用されるファイルキーであって、前記暗号化キーで暗号化される、ファイルキーを識別し、

前記ファイルキーを前記復号キーで復号し、

前記暗号化ファイルを前記ファイルキーで復号することによって前記暗号化ファイルにアクセスするようにプログラムされる、請求項１１に記載のシステム。

【発明の詳細な説明】

【背景技術】

【０００１】

組織及び消費者が第三者サービスを使用してデータを記憶することが増えている。第三者記憶サービスは、柔軟性、低資本金、アドオンサービス、データ共有、及びデータへの集中型アクセスを含む、多数の利点を顧客に提供することができる。

【０００２】

多くの第三者記憶の顧客は、データを第三者記憶業者に提出する前にそのデータを暗号化することを望むか、又はそれを行う必要がある。例えば、個人消費者は、プライバシーに対する懸念により第三者記憶業者に送信されるデータを暗号化することを望む場合がある。同様に、組織は、政府による法令、他の組織とのパートナーシップ契約書等の内部又は外部のデータ保護要件の順守を確実にするために、第三者記憶業者に送信されるデータを暗号化することを望む場合がある。残念ながら、データを第三者記憶システムに提出する前にそのデータを暗号化することによって、顧客は、データを重複排除する第三者記憶業者の試みを妨げる場合がある。例えば、２人の顧客が異なる暗号化方式（例として、異なるキー）を用いて同一のファイルを暗号化する場合、結果として得られる暗号化ファイルは異なるものとなり、第三者記憶業者がそのファイルを重複排除して、複数回参照される単一ファイルにするのを防ぐ可能性がある。加えて、第三者記憶システムに提出する前にファイルを暗号化することは、ファイルにセキュリティ走査を実施すること、ファイルのカスタムビューを生成することなど、対象とされる他のユーザとファイルを効率的に共有する、及び／又はファイルに他のサービスを実施する第三者記憶サービスの能力を妨げる場合がある。

【発明の概要】

【発明が解決しようとする課題】

【０００３】

上記の制限を考慮して、本開示は、安全な第三者データ記憶のための追加及び改善されたシステム及び方法の必要性を特定する。

【課題を解決するための手段】

【０００４】

本開示は、概して、安全な第三者データ記憶のためのシステム及び方法に関する。より詳細に後述されるように、安全化されたデータ（例えば、ファイル及び／又はファイルの暗号化キー）を暗号化及び復号するための非対称キーペアを第三者記憶サーバ上に維持し、これらの非対称キーペアの復号キーをクライアントによって維持される暗号化キーで暗号化することによって、本明細書に記載されるシステム及び方法は、第三者記憶サーバが必要に応じてデータを暗号化するのを可能にするが、安全化されたデータにアクセスするためには、クライアントが復号キーを提出することを必要とすることができる。

【０００５】

一実施形態では、安全な第三者データ記憶のためのコンピュータ実装方法は、１）サーバ側コンピューティングデバイスで、ユーザアカウントの下に記憶された暗号化ファイルにアクセスするクライアントシステムからの要求を識別すること（要求されたアクセスが暗号化ファイルの復号を必要とする）と、２）要求に応答して、暗号化キーと、クライアント側キーで暗号化されている復号キーとを含むユーザアカウントに指定された非対称キーペアを識別することと、３）クライアントシステムから、クライアント側キーを受信することと、４）復号キーをクライアント側キーで復号することと、５）復号キーを使用して、暗号化ファイルの暗号化されていないバージョンにアクセスすることとを含むことができる。

【０００６】

いくつかの例では、クライアント側キーを受信することは、クライアント側キーを不揮発性メモリ内に記憶することなくクライアント側キーを揮発性メモリ内に記憶することを含むことができる。復号キーを使用して、暗号化ファイルの暗号化されていないバージョンにアクセスすることは、多様な工程のうちのいずれかを含むことができる。いくつかの実施形態では、復号キーを使用して、暗号化ファイルの暗号化されていないバージョンにアクセスすることは、１）暗号化ファイルを暗号化するために使用されるファイルキー（暗号化キーで暗号化されている）を識別することと、２）ファイルキーを復号キーで復号することと、３）暗号化ファイルをファイルキーで復号することとを含むことができる。

【０００７】

いくつかの例では、復号キーを使用して、暗号化ファイルの暗号化されていないバージ

ョンにアクセスすることは、暗号化ファイルの暗号化されていないバージョンを記述するメタデータを生成することを含むことができる。これらの例では、メタデータを生成することは、１）暗号化ファイルの暗号化されていないバージョンのセキュリティ走査を実施すること、２）暗号化ファイルの暗号化されていないバージョン内のコンテンツに基づいて、暗号化ファイルの暗号化されていないバージョンを索引付けすること、及び／又は３）暗号化ファイルの暗号化されていないバージョンのプレビューを生成することを含むことができる。

【０００８】

いくつかの実施形態では、復号キーを使用して、暗号化ファイルの暗号化されていないバージョンにアクセスすることは、１）ユーザアカウントを含む複数のユーザアカウントに指定された追加の非対称キーペアであって、追加の暗号化キーと、暗号化キーで暗号化されている追加の復号キー（例えば、ユーザアカウントに指定された非対称キーペアの追加の復号キー）とを含む、非対称キーペアを識別することと、２）追加の復号キーを復号キー（例えば、ユーザアカウントに指定された非対称キーペアの復号キー）で復号することと、３）暗号化ファイルを暗号化するために使用されるファイルキー（追加の暗号化キーで暗号化されている）を識別することと、４）ファイルキーを追加の復号キーで復号することと、５）暗号化ファイルをファイルキーで復号することとを含むことができる。

【０００９】

いくつかの例では、暗号化ファイルの暗号化されていないバージョンにアクセスすることは、暗号化ファイルの暗号化されていないバージョンをクライアントシステムに送信することを含むことができる。加えて、又は代替として、暗号化ファイルの暗号化されていないバージョンにアクセスすることは、暗号化ファイルの暗号化されていないバージョンへのアクセスを追加のユーザアカウントに提供することであって、１）追加の非対称キーペアが追加のユーザアカウントに指定され、２）追加の非対称キーペアが追加の暗号化キーと、追加の復号キーとを含み、かつ３）追加の復号キーが追加のクライアント側キーで暗号化される、追加のユーザアカウントに提供することを含むことができる。これらの実施形態では、暗号化ファイルの暗号化されていないバージョンへのアクセスを追加のユーザアカウントに提供することは、１）暗号化ファイルを暗号化するために使用されるファイルキー（暗号化キーで暗号化されている）を識別することと、２）ファイルキーを復号キーで復号することと、３）ファイルキーのコピーを追加の暗号化キーで暗号化することとを含むことができる。

【００１０】

いくつかの例では、コンピュータ実装方法はまた、１）暗号化ファイルの暗号化されていないバージョンにアクセスするように指定された追加のユーザアカウントを識別することであって、ａ）追加の非対称キーペアが、追加のユーザアカウントに指定され、ｂ）追加の非対称キーペアが、追加の暗号化キーと、追加の復号キーとを含み、ｃ）追加の復号キーが追加のクライアント側キーで暗号化される、追加のユーザアカウントを識別することと、２）復号キーを追加の暗号化キーで暗号化することとを含むことができる。これらの例では、コンピュータ実装方法は、１）追加のユーザアカウントを介して暗号化ファイルに更にアクセスする追加のクライアントシステムからの追加の要求を識別すること（追加の要求されたアクセスが暗号化ファイルの復号を必要とする）と、２）復号キーを追加の復号キーで復号することと、３）復号キーを使用して、追加のユーザアカウントを介して暗号化ファイルの暗号化されていないバージョンにアクセスすることとを更に含むことができる。

【００１１】

一例では、コンピュータ実装方法はまた、１）クライアントシステムから暗号化ファイルの暗号化されていないバージョンを受信することと、２）暗号化ファイルを、ａ）暗号化ファイルの暗号化されていないバージョンの少なくとも１つの特性に基づいてファイルキーを生成し、ｂ）暗号化ファイルの暗号化されていないバージョンをファイルキーで暗号化することによって生成することと、３）ファイルキーを暗号化キーで暗号化すること

とを含むことができる。この例では、コンピュータ実装方法は、暗号化ファイルを、ファイルキーで暗号化される追加の暗号化ファイルで重複排除することを更に含むことができる。

【００１２】

一実施形態では、上記の方法を実装するためのシステムは、１）サーバ側コンピューティングデバイスで、ユーザアカウントの下に記憶された暗号化ファイルにアクセスするクライアントシステムからの要求を識別するようにプログラムされる識別モジュール（要求されたアクセスが暗号化ファイルの復号を必要とする）と、２）要求に応答して、暗号化キーと、クライアント側キーで暗号化されている復号キーとを含むユーザアカウントに指定された非対称キーペアを識別するようにプログラムされるキーモジュールと、３）クライアントシステムから、クライアント側キーを受信するようにプログラムされる受信モジュールと、４）復号キーをクライアント側キーで復号するようにプログラムされる復号モジュールと、５）復号キーを使用して、暗号化ファイルの暗号化されていないバージョンにアクセスするようにプログラムされるアクセスモジュールとを含み得る。本システムはまた、識別モジュール、キーモジュール、受信モジュール、復号モジュール、及びアクセスモジュールを実行するように構成される、少なくとも１つのプロセッサを含み得る。

【００１３】

一部の実施例において、上記に説明される方法は、コンピュータで読み取り可能な記憶媒体上に、コンピュータで読み取り可能な命令としてコード化され得る。例えば、コンピュータ読み取り可能な記憶媒体は、コンピューティングデバイスの少なくとも１つのプロセッサによって実行されるとき、コンピューティングデバイスに、１）サーバ側コンピューティングデバイスで、ユーザアカウントの下に記憶された暗号化ファイルにアクセスするクライアントシステムからの要求を識別すること（要求されたアクセスが暗号化ファイルの復号を必要とし）と、２）要求に応答して、暗号化キーと、クライアント側キーで暗号化されている復号キーとを含むユーザアカウントに指定された非対称キーペアを識別することと、３）クライアントシステムから、クライアント側キーを受信することと、４）復号キーをクライアント側キーで復号することと、５）復号キーを使用して、暗号化ファイルの暗号化されていないバージョンにアクセスすることと、を行わせることができる、１つ以上のコンピュータ実行可能な命令を含み得る。

【００１４】

下記により詳細に説明されるように、安全化されたデータを暗号化及び復号するための非対称キーペアを第三者記憶サーバ上に維持し、非対称キーペアの復号キーをクライアントによって維持される暗号化キーで暗号化することによって、本明細書に記載されるシステム及び方法は、暗号化されていない状態で、安全化されたデータにアクセスするために必要なクライアント側復号キーを記憶することなく、クライアントデータを安全に記憶及び暗号化することができる。それにより、これらのシステム及び方法は、第三者記憶システムへのアクセスを得た攻撃者が、暗号化されていない状態の安全化されたデータにアクセスするのを防ぐことができ、同時に、この安全化されたデータの共有、重複排除、分析、及び／又は索引付けを更に可能にする、及び／又は容易にする。

【００１５】

上に記述される実施形態のうちのいずれかからの特性は、本明細書に記載の一般原理に従って、互いに組み合わせて使用されてもよい。これら及び他の実施形態、特性、及び利点は、添付の図面及び特許請求の範囲と共に以下の詳細な説明を一読することでより完全に理解されるであろう。

【図面の簡単な説明】

【００１６】

添付の図面は、多数の例示的な実施形態を例解し、かつ本明細書の一部である。以下の説明と共に、これらの図面は、本開示の多様な原理を例証及び説明する。

【図１】安全な第三者データ記憶のための例示的なシステムのブロック図である。

【図２】安全な第三者データ記憶のための例示的なシステムのブロック図である。

【図３】安全な第三者データ記憶のための例示的な方法の流れ図である。
【図４】安全な第三者データ記憶のための例示的なシステムのブロック図である。
【図５】安全な第三者データ記憶のための例示的なシステムのブロック図である。
【図６】安全な第三者データ記憶のための例示的なシステムのブロック図である。
【図７】安全な第三者データ記憶のための例示的なシステムのブロック図である。
【図８】本明細書に記載及び／又は例解される実施形態のうちの１つ以上を実装することが可能な例示的なコンピューティングシステムのブロック図である。
【図９】本明細書に記載及び／又は例解される実施形態のうちの１つ以上を実装することが可能な例示的なコンピューティングネットワークのブロック図である。
【００１７】
図面を通して、同一の参照文字及び説明は、類似しているが必ずしも同一ではない要素を示す。本明細書に記載の例示的な実施形態は多様な修正及び代替形態が可能であるが、具体的な実施形態が、図面において例として示されており、本明細書に詳細に説明されるであろう。しかしながら、本明細書に記載の例示的な実施形態は、開示される特定の形態に限定されることを意図するものではない。むしろ、本開示は、添付の特許請求の範囲内にある全ての修正、同等物、及び代替物を網羅する。
【発明を実施するための形態】
【００１８】
図１～２及び４～７を参照することにより、以下に安全な第三者データ記憶のための例示的なシステムの詳細な説明が提供される。対応するコンピュータ実装方法の詳細な説明はまた、図３と併せて提供される。更に、本明細書に記載の実施形態のうちの１つ以上を実装することが可能な例示的なコンピューティングシステム及びネットワークアーキテクチャの詳細な説明は、それぞれに、図８及び９と併せて提供される。
【００１９】
図１は、安全な第三者データ記憶のための例示的なシステム１００のブロック図である。この図に例解されるように、例示的なシステム１００は、１つ以上のタスクを実施するための１つ以上のモジュール１０２を含み得る。例えば、下記により詳細に説明されるように、例示的なシステム１００は、サーバ側コンピューティングデバイスで、ユーザアカウントの下に記憶された暗号化ファイルにアクセスするクライアントシステムからの要求を識別するようにプログラムされる識別モジュール１０４を含むことができる。例示的なシステム１００はまた、暗号化キーと、クライアント側キーで暗号化されている復号キーとを含む、ユーザアカウントに指定された非対称キーペアを識別するようにプログラムされるキーモジュール１０６を含み得る。
【００２０】
加えて、下記により詳細に記載されるように、例示的なシステム１００は、クライアントシステムからクライアント側キーを受信するようにプログラムされる受信モジュール１０８を含むことができる。例示的なシステム１００は、復号キーをクライアント側キーで復号するようにプログラムされる復号モジュール１１０を含むことができる。例示的なシステム１００は、復号キーを使用して、暗号化ファイルの暗号化されていないバージョンにアクセスするようにプログラムされるアクセスモジュール１１２を含むことができる。別個の要素として例解されるが、図１のモジュール１０２のうちの１つ以上は、単一のモジュール又はアプリケーションの部分を表し得る。
【００２１】
ある実施形態において、図１のモジュール１０２のうちの１つ以上は、コンピューティングデバイスにより実行されるとき、コンピューティングデバイスに１つ以上のタスクを実施させ得る、１つ以上のソフトウェアアプリケーション又はプログラムを表し得る。例えば、下記により詳細に記載されるように、モジュール１０２のうちの１つ以上は、図２に例解されるデバイス（例えば、コンピューティングデバイス２０２及び／又はクライアントシステム２０６）、図８のコンピューティングシステム８１０、及び／又は図９の例示的なネットワークアーキテクチャ９００の部分等、１つ以上のコンピューティングデバ

イスに記憶され、そこで作動するように構成されるソフトウェアモジュールを表し得る。図１のモジュール１０２のうちの１つ以上はまた、１つ以上のタスクを実施するように構成される、１つ以上の特殊目的のコンピュータの全て又は部分を表し得る。

【００２２】

図１の例示的なシステム１００は、多様な方法で実装されてもよい。例えば、例示的なシステム１００の全て又は一部分は、図２の例示的なシステム２００の部分を表し得る。図２に示されるように、システム２００は、ネットワーク２０４を介してクライアントシステム２０６と通信する（例えば、第三者記憶サービスをクライアントシステム２０６に提供する）コンピューティングデバイス２０２を含むことができる。

【００２３】

一実施形態では、図１のモジュール１０２のうちの１つ以上は、コンピューティングデバイス２０２の少なくとも１つのプロセッサによって実行されるとき、安全な第三者データ記憶内でコンピューティングデバイス２０２を容易にすることができる。例えば、下記により詳細に記載されるように、モジュール１０２のうちの１つ以上は、コンピューティングデバイス２０２に、１）サーバ側コンピューティングデバイス２０２で、ユーザアカウント２４０の下に記憶された暗号化ファイル２４２にアクセスするクライアントシステム２０６からの要求２１０を識別すること、２）要求２１０に応答して、暗号化キー２２２と、クライアント側キー２３０で暗号化されている暗号化された復号キー２２４とを含むユーザアカウント２４０に指定された非対称キーペア２２０を識別すること、３）クライアントシステム２０６からクライアント側キー２３０を受信すること、４）暗号化された復号キー２２４をクライアント側キー２３０で復号すること（例えば、復号キー２２６をもたらすこと）、５）復号キー２２６を使用して、暗号化ファイル２４２（例えば、ファイル２４４）の暗号化されていないバージョンにアクセスすること、を行わせることができる。

【００２４】

コンピューティングデバイス２０２及びクライアントシステム２０６は概して、コンピュータ実行可能な命令を読み取ることが可能な任意のタイプ又は形態のコンピューティングデバイスを表す。コンピューティングデバイス２０２及びクライアントシステム２０６の例としては、これらに限定されないが、サーバ、デスクトップ、ラップトップ、タブレット、携帯電話、携帯情報端末（ＰＤＡ）、マルチメディアプレーヤ、埋め込みシステム、これらのうちの１つ以上の組み合わせ、図８の例示的なコンピューティングシステム８１０、又は任意の他の好適なコンピューティングデバイスが挙げられる。

【００２５】

ネットワーク２０４は、概して、通信又はデータ転送を容易にすることが可能な任意の媒体又はアーキテクチャを表す。ネットワーク２０４の例としては、これらに限定されないが、イントラネット、広域ネットワーク（ＷＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、パーソナルエリアネットワーク（ＰＡＮ）、インターネット、電力線通信（ＰＬＣ）、セルラーネットワーク（例えば、ＧＳＭネットワーク（「ＧＳＭ」は登録商標））、図９の例示的なネットワークアーキテクチャ９００、等が挙げられる。ネットワーク２０４は、無線又は有線接続を使用して通信又はデータ転送を容易にし得る。一実施形態では、ネットワーク２０４は、コンピューティングデバイス２０２とクライアントシステム２０６との間の通信を容易にすることができる。

【００２６】

図３は、安全な第三者データ記憶のための例示的なコンピュータ実装方法３００の流れ図である。図３に示される工程は、任意の好適なコンピュータで実行可能なコード及び／又はコンピューティングシステムにより実施されてもよい。一部の実施形態において、図３に示される工程は、図１のシステム１００の構成要素のうちの１つ以上、図２のシステム２００、図８のコンピューティングシステム８１０、及び／又は図９の例示的なネットワークアーキテクチャ９００の部分により実施されてもよい。

【００２７】

図３に例解されるように、工程３０２では、本明細書に記載されるシステムのうちの１つ以上は、サーバ側コンピューティングデバイスで、ユーザアカウントの下に記憶された暗号化ファイルにアクセスするクライアントシステムからの要求を識別することができる。例えば、工程３０２では、識別モジュール１０４は、図２のコンピューティングデバイス２０２の一部として、ユーザアカウント２４０の下に記憶された暗号化ファイル２４２にアクセスするクライアントシステム２０６からの要求２１０を識別することができる。上記の例のいずれにおいても、要求されたアクセスは、暗号化ファイルの復号を必要とするか又はそれを伴い得る。

【００２８】

いくつかの例では、サーバ側コンピューティングデバイスは、第三者記憶システムの一部として動作することができる。本明細書で使用されるとき、用語「第三者記憶システム」は、ユーザの代わりにデータを記憶することが可能であるクラウドベースの記憶システムを含む任意のタイプ又は形態の記憶システムを指す。いくつかの例では、第三者記憶システムは、多数の異なる実体のデータを記憶することができる。少なくとも１つの例では、第三者記憶システムでデータを記憶する実体は、互いに（例えば、実体を超えるデータの非特権アクセスを防ぐために）、侵入者（例えば、第三者記憶システム内に記憶されたデータにアクセスする権限を付与されていない実体）、及び／又は第三者記憶システムの１人以上の管理者に対してデータの安全性を必要とし得る。いくつかの例では、第三者記憶システムは、単一インスタンスの記憶システム（即ち、多数の所有者のコンテンツの各項目の単一インスタンスのみ記憶するように構成される記憶システム）を表すか又は含むことができる。

【００２９】

したがって、クライアントシステムは、同様に、第三者記憶システムの使用を容易にするための任意のシステムを含むことができる。いくつかの例では、クライアントシステムは、サーバ側コンピューティングデバイスの所有者及び／又は管理者とは異なる実体によって所有及び／又は管理されてもよい。

【００３０】

本明細書で使用されるとき、用語「ファイル」は、これらに限定されないが、ファイル、データオブジェクト、データセグメント、データストリームの部分、データベース、データベース入力、及び／又は電子文書を含む任意の好適な単位のデータを指すことができる。加えて、語句「ユーザアカウント」は、データ所有者に対応し得る任意の識別子及び／又は特権システム（例えば、データ所有者によって所有されるデータを識別する、及び／又はデータ所有者による使用のためにデータ所有者によって所有されるデータを確保するために使用される）を指すことができる。

【００３１】

識別モジュール１０４は、多様なタイプの要求のうちのいずれかを識別することができる。例えば、下記により詳細に説明されるように、識別モジュール１０４は、クライアントシステムのための暗号化ファイルの暗号化されていないバージョンを取り出す要求を識別することができる。加えて、又は代替として、識別モジュール１０４は、ファイルのアクセス可能なバージョンを別のユーザアカウントと共有する要求を識別することができる。いくつかの例では、識別モジュール１０４は、ファイルに１つ以上のプロシージャ（例えば、暗号化ファイルの暗号化されていないバージョンへのアクセスを必要とするプロシージャ）を実施する要求を識別することができる。

【００３２】

識別モジュール１０４は、多様なコンテクストのうちのいずれかにおける要求を受信することができる。例えば、識別モジュール１０４は、クライアントシステムからユーザ起動要求を受信することができる。加えて、又は代替として、下記により詳細に説明されるように、識別モジュール１０４は、暗号化ファイルへのアクセスを可能にするクライアントシステムからクライアント側キーを単純に受信することによって暗号化ファイルにアクセスする暗黙の要求を受信することができる。

【００３３】
図３に戻り、工程３０４では、本明細書に記載されるシステムのうちの１つ以上は、要求に応答して、暗号化キーと、クライアント側キーで暗号化されている復号キーとの両方を含むユーザアカウントに指定された非対称キーペアを識別することができる。例えば、工程３０４では、キーモジュール１０６は、図２のコンピューティングデバイス２０２の一部として、要求２１０に応答して、暗号化キー２２２と、クライアント側キー２３０で暗号化されている暗号化された復号キー２２４との両方を含むユーザアカウント２４０に指定された非対称キーペア２２０を識別することができる。
【００３４】
本明細書で使用されるとき、語句「非対称キーペア」は、暗号化キー（又は「公開キー」）及び復号キー（又は「秘密キー」）の両方を含む暗号キーの任意のペアを指すことができる。暗号化キーは、キーで暗号化されたデータを安全化するために秘密性を必要としないあらゆるキーを含み得る。例えば、暗号化キーは、非対称キーアルゴリズムを用いてデータを暗号化するために使用されてもよい。その結果として、暗号化キーで暗号化されたデータを復号することは、非対称キーペアの対応する復号キーを必要とし得る。いくつかの例では、非対称キーペアは、第三者記憶システム上、及び／又はそれによって記憶されてもよい。少なくとも１つの例では、暗号化キーも復号キーも第三者記憶システムの外側に分配され得ない。
【００３５】
加えて、語句「クライアント側キー」は、本明細書で使用されるとき、任意の好適な暗号キー、又は非対称キーペアの復号キーを暗号化及び／若しくは復号するためのキーを指すことができる。いくつかの例では、クライアント側キーは、対称キー（例えば、データを暗号化すること、及び前記データを復号することの両方に使用可能なキー）を含み得る。例えば、クライアント側キーは、ＡＥＳ（Advanced Encryption Standard）仕様書（例えば、ＡＥＳ－２５６）に従ってデータを暗号化及び復号するように構成されてもよい。いくつかの例では、クライアント側キーは、クライアントシステム上で生成されてもよい。例えば、クライアント側キーは、パスワードベースのキー導出関数（例えば、ＰＢＫＤＦ２）等のキー導出関数を用いて生成されてもよい。
【００３６】
いくつかの例では、クライアント側キーは、クライアントシステムにキャッシュされ得る。加えて、又は代替として、クライアント側キーは、パスワードから必要に応じて生成され（例えば、クライアントシステム又は第三者記憶システムのいずれかで生成され）てもよい。いくつかの例では、クライアント側キーは、外部キーストアから取り出されてもよい。下記により詳細に説明されるように、いくつかの例では、クライアント側キーは、サーバ側コンピューティングデバイス上、及び／又はサーバ側コンピューティングデバイスによって実装される第三者記憶システム内に記憶されない場合がある。いくつかの例では、クライアント側キーは、対応するクライアントによってのみアクセス可能であってもよい。このクライアントは、組織、共有された秘密を有するグループ、コンピューティングデバイス、及び／又は任意の他の好適な実体に相当し得る。
【００３７】
いくつかの例では、本明細書に記載されるシステムのうちの１つ以上は、非対称キーペア内の暗号化キーを使用して、暗号化ファイルを暗号化した可能性がある。例えば、本明細書に記載されるシステムのうちの１つ以上は、クライアントシステムから暗号化ファイルの暗号化されていないバージョンを受信し、次いで暗号化ファイルを生成することができる。これらのシステムは、暗号化ファイルの暗号化されていないバージョンの少なくとも１つの特性に基づいてファイルキーを生成し、次いで、ファイルキーで、暗号化ファイルの暗号化されていないバージョンを暗号化することによって生成することができる。例えば、これらのシステムは、暗号化ファイルの暗号化されていないバージョンのハッシュを導出し、ハッシュをファイルキーの基礎とすることができる。このように、本明細書に記載されるシステム及び方法は、同一の暗号化されていないファイルから同一の暗号化フ

ァイルを生成し、クライアントにわたる重複排除を可能にすることができる。
【００３８】
例えば、本明細書に記載されるシステムは、暗号化ファイルに、ファイルキーで暗号化される追加の暗号化ファイルとの重複排除を行うことができる。ファイルキーを生成すると、これらのシステムは、ファイルキーを暗号化キーで暗号化することができる。用語「重複排除」は、本明細書で使用されるとき、データが単一インスタンスデータ記憶システムに重複して記憶されるのを検出及び防止するための動作を含む、単一インスタンスデータ記憶システムに使用される記憶領域の量を減少させることに関する１つ以上の動作を指すことができる。重複排除は、任意の好適な重複排除技術又はアルゴリズムを用いて実施され得る。いくつかの例では、重複排除は、ファイルレベルの重複排除を含み得る。加えて、又は代替として、重複排除は、ブロックレベルの重複排除を含んでもよい。
【００３９】
暗号化ファイルの暗号化されていないバージョンを暗号化することに加えて、いくつかの例では、本明細書に記載されるシステムのうちの１つ以上は、暗号化ファイルの暗号化されていないバージョンに基づいて（例えば、暗号化ファイルの暗号化されていないバージョンを暗号化し、それにより暗号化ファイルの暗号化されていないバージョンへのアクセスを失う前に）、１つ以上の動作を実施することができる。例えば、本明細書に記載されるシステムのうちの１つ以上は、暗号化ファイルの暗号化されていないバージョンのコンテンツを索引付けし、暗号化ファイルの暗号化されていないバージョンにアンチマルウェア走査を実施し、暗号化ファイルの暗号化されていないバージョンのコンテンツのプレビューを生成するなどを行うことができる。これらの例では、これらのシステムは、暗号化ファイルが暗号化された時点で、暗号化ファイルの暗号化されていないバージョンから生成されたメタデータを暗号化ファイルと関連付けることができる。
【００４０】
キーモジュール１０６は、任意の好適な様式でユーザアカウントに指定された非対称キーペアを識別することができる。いくつかの例では、第三者記憶システムは、各々が、指定された異なる非対称キーペアを有する、複数のユーザアカウントのデータをホストすることができる。したがって、キーモジュール１０６は、クライアントシステムによって提供される１つ以上の識別子及び／又は認証情報に従ってユーザアカウントの非対称キーペアを識別することができる。
【００４１】
図３に戻り、工程３０６では、本明細書に記載されるシステムのうちの１つ以上は、クライアントシステムから、クライアント側キーを受信することができる。例えば、工程３０６では、受信モジュール１０８は、図２のコンピューティングデバイス２０２の一部として、クライアントシステム２０６からクライアント側キー２３０を受信することができる。
【００４２】
前述のように、いくつかの例では、クライアント側キーは、サーバ側に（即ち、サーバ側コンピューティングデバイス及び／又は関連付けられた第三者記憶システムに）記憶されない場合がある。例えば、受信モジュール１０８は、クライアント側キーを受信し、クライアント側キーを不揮発性メモリ内に記憶することなくクライアント側キーを揮発性メモリ内に記憶することができる。本明細書で使用されるとき、語句「揮発性メモリ」は、あらゆる非持続的及び／又は一時的記憶場所を指すことができる。いくつかの例では、語句「揮発性メモリ」は、ランダムアクセスメモリを指すことができる。加えて、語句「不揮発性メモリ」は、あらゆる持続的記憶場所を指すことができる。例えば、語句「不揮発性メモリ」は、１つ以上のファイルを記憶するためにファイルシステムによって使用される記憶デバイスを指すことができる。いくつかの例では、受信モジュール１０８は、クライアント側キーを受信することができ、使用後にはクライアント側キーを保存しなくてもよい。例えば、受信モジュール１０８は、クライアントシステムとのセッションが終了した後、クライアント側キーを破棄することができる。

【００４３】
受信モジュール１０８は、多様な方法のうちのいずれかでクライアントシステムからクライアント側キーを受信することができる。例えば、受信モジュール１０８は、クライアントシステムから直接クライアント側キーを受信することができる。加えて、又は代替として、受信モジュール１０８は、クライアント側キーを表すデータを受信することによってクライアントシステムからクライアント側キーを受信することができ、そこからクライアント側キーが生成され得る。例えば、受信モジュール１０８は、クライアントシステムからキー導出関数のパスワードを受信し、このキー導出関数を使用して、パスワードからクライアント側キーを生成することができる。この例では、受信モジュール１０８はまた、パスワードを不揮発性メモリ内にのみ保存し、及び／又はパスワードを使用して、クライアント側キーを生成するとパスワードを破棄することができる。

【００４４】
図３に戻り、工程３０８では、本明細書に記載されるシステムのうちの１つ以上は、復号キーをクライアント側キーで復号することができる。例えば、工程３０８では、復号モジュール１１０は、図２のコンピューティングデバイス２０２の一部として、暗号化された復号キー２２４をクライアント側キー２３０で復号する（例えば、復号キー２２６をもたらす）ことができる。

【００４５】
復号モジュール１１０は、復号キーを任意の好適な様式で復号することができる。例えば、復号モジュール１１０は、復号キーの復号化されたバージョンを生成する所定の対称キーアルゴリズムに従って、クライアント側キーを復号キーに適用することができる。

【００４６】
工程３１０では、本明細書に記載されるシステムのうちの１つ以上は、復号キーを使用して、暗号化ファイルの暗号化されていないバージョンにアクセスすることができる。例えば、工程３１０では、アクセスモジュール１１２は、図２のコンピューティングデバイス２０２の一部として、復号キー２２６を使用して、暗号化ファイル２４２の暗号化されていないバージョン（例えば、ファイル２４４）にアクセスすることができる。

【００４７】
アクセスモジュール１１２は、多様な方法のいずれかで、復号キーを使用して、暗号化ファイルの暗号化されていないバージョンにアクセスすることができる。例えば、アクセスモジュール１１２は、暗号化ファイルを暗号化するために使用されるファイルキーを識別することができる。この例では、ファイルキーは、暗号化キーで暗号化され得る。したがって、アクセスモジュール１１２は、ファイルキーを復号キーで復号し、次いで暗号化ファイルをファイルキーで復号することができる。

【００４８】
アクセスモジュール１１２は、多様な目的のいずれかに対して暗号化ファイルの暗号化されていないバージョンにアクセスすることができる。例えば、上記に詳述されるように、クライアントシステムからの要求は、暗号化ファイルの暗号化されていないバージョンを取り出す要求を含むことができる。したがって、アクセスモジュール１１２は、暗号化ファイルの暗号化されていないバージョンをクライアントシステムに（例えば、要求に応答して）送信することができる。

【００４９】
図４は、安全な第三者データ記憶のための例示的なシステム４００を例解する。図４に示されるように、例示的なシステム４００は、第三者記憶サーバ４２０によって容易にされる第三者記憶サービスを介して１つ以上のファイルを記憶するように構成されるクライアントシステム４１０を含むことができる。例えば、クライアントシステム４１０は、暗号化されていないファイル４４６を第三者記憶サーバ４２０に以前に送信した可能性がある。第三者記憶サーバ４２０は、クライアントシステム４１０と関連付けられた非対称キーペア４３０を識別し、暗号化キー４３２を用いて暗号化されていないファイル４４６を暗号化した可能性がある。一例では、クライアントシステム４１０は、現時点では暗号化

ファイル４４０として第三者記憶サーバ４２０に記憶されている、暗号化されていないファイル４４６を取り出すことを試みることができる。例えば、工程４５０では、クライアントシステム４１０は、暗号化されていないファイル４４６を要求し、クライアント側キー４１２を含むメッセージを第三者記憶サーバ４２０に送信することができる。第三者記憶サーバ４２０は、それに応じて、クライアント側キー４１２を受信し、クライアント側キー４１２を使用のためにメモリ内に維持することができる。

【００５０】

工程４５２では、第三者記憶サーバ４２０は、非対称キーペア４３０を識別し、暗号化された復号キー４３４をクライアント側キー４１２を用いて復号して、復号キー４３６をもたらすことができる。工程４５４では、第三者記憶サーバ４２０は、復号キー４３６を使用して、暗号化されたファイルキー４４２を復号し、暗号化ファイル４４０のファイルキー４４４を得ることができる。工程４５６では、第三者記憶サーバ４２０は、ファイルキー４４４を使用して、暗号化ファイル４４０を復号し、暗号化されていないファイル４４６を得ることができる。工程４５８では、第三者記憶サーバ４２０は、暗号化されていないファイル４４６をクライアントシステム４１０に送信し、クライアントシステム４１０による要求を満たすことができる。加えて、第三者記憶サーバ４２０は、クライアント側キー４１２、復号キー４３６、及びファイルキー４４４を破棄し、暗号化されていないファイル４４６を削除することができる。

【００５１】

図３の工程３１０に戻り、いくつかの例では、アクセスモジュール１１２は、暗号化ファイルの暗号化されていないバージョンにアクセスして、暗号化ファイルの暗号化されていないバージョンを記述するメタデータを生成することができる。いくつかの例では、アクセスモジュール１１２は次に、暗号化ファイルの暗号化されていないバージョンがもはや第三者記憶システムで直接アクセスできなくなった後であっても、暗号化ファイルを記述したメタデータは利用可能なままであるように、メタデータを暗号化ファイルと関連して記憶することができる。

【００５２】

例えば、アクセスモジュール１１２は、（例えば、暗号化ファイルが何らかのマルウェアを含むか、又は何らかの他のセキュリティリスクをもたらすかを判定するために）暗号化ファイルの暗号化されていないバージョンにセキュリティ走査を実施することができる。別の例では、アクセスモジュール１１２は、暗号化ファイルの暗号化されていないバージョン内のコンテンツに基づいて暗号化ファイルの暗号化されていないバージョンを索引付けする（例えば、暗号化ファイルの暗号化されていないバージョンへアクセスすることなくそのコンテンツに基づいて暗号化ファイルを探すのを容易にする）ことができる。更なる例では、アクセスモジュール１１２は、暗号化ファイルの暗号化されていないバージョン内のコンテンツに基づいて暗号化ファイルの暗号化されていないバージョンのプレビューを生成する（例えば、暗号化ファイルの暗号化されていないバージョンへアクセスすることなく暗号化ファイルを閲覧するのを容易にする）ことができる。加えて、又は代替として、上記に詳述されるように、いくつかの例では、本明細書に記載される１つ以上のシステムは、暗号化ファイルの暗号化されていないバージョンが最初にアップロードされるときに（例えば、暗号化前に）、上述される動作のうちの１つ以上を実施することができる。

【００５３】

いくつかの例では、アクセスモジュール１１２は、暗号化ファイルの暗号化されていないバージョンへのアクセスを別の関係者に提供することができる。例えば、アクセスモジュール１１２は、暗号化ファイルの暗号化されていないバージョンへのアクセスを別のユーザアカウントに提供することができる。この例では、追加の非対称キーペアは、追加の暗号化キーと、追加の復号キーとを含む追加のユーザアカウントに指定されてもよい。追加の復号キーは、追加のクライアント側キー（例えば、追加のユーザアカウントに対応する追加のクライアントシステムに関連する）で暗号化されてもよい。この例では、アクセ

スモジュール１１２は、暗号化ファイルを暗号化するために使用されるファイルキーを最初に識別することによって暗号化ファイルの暗号化されていないバージョンへのアクセスを追加のユーザアカウントに提供することができる。暗号化ファイルがユーザアカウントに関連し得ることにより、ファイルキーは、暗号化キー（即ち、ユーザアカウントに対応する非対称キーペアの暗号化キー）で暗号化されてもよい。アクセスモジュール１１２は次に、ファイルキーを復号キーで復号し、ファイルキーのコピーを追加の暗号化キーで暗号化することができる。このように、追加のユーザアカウントは、暗号化ファイルへのアクセス（例えば、追加のクライアント側キーを提出してファイルキーを復号し、ファイルキーによる暗号化ファイルの復号を可能にすることによる）を有することができる。

【００５４】

図５は、安全な第三者データ記憶のための例示的なシステム５００を例解する。図５に示されるように、例示的なシステム５００は、第三者記憶サーバ５２０によって容易にされた第三者記憶サービスを介して１つ以上のファイルを記憶し、及び／又はそれにアクセスするように構成されるクライアントシステム５１０（１）及び５１０（２）を含むことができる。例えば、第三者記憶サーバ５２０は、クライアントシステム５１０（１）の代わりに暗号化ファイル５４０を記憶することができる。この例では、非対称キーペア５３０（１）は、クライアントシステム５１０（１）に対応することができ、非対称キーペア５３０（２）は、クライアントシステム５１０（２）に対応することができる。したがって、暗号化ファイル５４０は、暗号化キー５３２（１）で暗号化されるファイルキー５４４で暗号化され、暗号化されたファイルキー５４２（１）として記憶されてもよい。

【００５５】

工程５５０では、クライアントシステム５１０（１）は、暗号化ファイル５４０の暗号化されていないコンテンツへのアクセスをクライアントシステム５１０（２）と共有する要求を第三者記憶サーバ５２０に送信することができる。この要求は、クライアント側キー５１２（１）を含むことができる。第三者記憶サーバ５２０は、クライアント側キー５１２（１）を受信し、工程５５２で、暗号化された復号キー５３４（１）をクライアント側キー５１２（１）で復号して、復号キー５３６（１）を得ることができる。工程５５４では、第三者記憶サーバ５２０は、暗号化されたファイルキー５４２（１）を復号キー５３６（１）で復号して、ファイルキー５４４を得ることができる。工程５５６では、第三者記憶サーバ５２０は、ファイルキー５４４を暗号化キー５３２（２）で暗号化して、暗号化されたファイルキー５４２（２）を得て、将来の使用のために暗号化されたファイルキー５４２（２）を記憶することができる。工程５５８では、第三者記憶サーバ５２０は、暗号化ファイル５４０の暗号化されていないコンテンツにアクセスするクライアントシステム５１０（２）からの要求を受信することができる。この要求は、クライアント側キー５１２（２）を含み、第三者記憶サーバ５２０が暗号化された復号キー５３４（２）を復号するのを可能にし、それによりファイルキー５４４を得て、暗号化ファイル５４０を復号するために暗号化されたファイルキー５４２（２）を復号することができる。

【００５６】

いくつかの例では、アクセスモジュール１１２は、追加のユーザアカウントに対応する追加のクライアント側キーがユーザアカウントの復号キーを復号するのを可能にすることによって、暗号化ファイルの暗号化されていないバージョンへのアクセスを追加のユーザアカウントに提供することができる。例えば、アクセスモジュール１１２は、暗号化ファイルの暗号化されていないバージョンにアクセスするように指定された追加のユーザアカウントを識別することができる。この例では、追加の非対称キーペアは、追加の暗号化キーと、追加の復号キーとの両方を含む追加のユーザアカウントに指定されてもよい。追加の復号キーは、追加のクライアント側キー（例えば、追加のユーザアカウントに対応する追加のクライアントシステムに関連する）で暗号化されてもよい。

【００５７】

上述の例では、アクセスモジュール１１２は、復号キーを追加の暗号化キーで暗号化すること（例えば、後の使用のために暗号化された復号キーを追加のユーザアカウントで記

憶すること）によって、暗号化ファイルの暗号化されていないバージョンへのアクセスを追加のユーザアカウントに提供することができる。例えば、本明細書に記載されるシステムのうちの１つ以上は、後で、追加のユーザアカウントを介して暗号化ファイルに更にアクセスする追加のクライアントシステムからの追加の要求を識別することができる。これらのシステムは次に、復号キーを追加の復号キーで復号し、この復号キーを使用して、追加のユーザアカウントを介して（例えば、この復号キーを使用して、暗号化ファイルが暗号化されたファイルキーを復号し、次いでこのファイルキーで暗号化ファイルを復号することによって）、暗号化ファイルの暗号化されていないバージョンにアクセスすることができる。いくつかの例では、上述される手法は、ユーザアカウントと追加のユーザアカウントとの間の多数のファイルを共有するために使用されてもよい。この手法はまた、いくつかの暗号処理工程を除外する（例えば、共有された各ファイルの別個の暗号化されたファイルキーの生成を必要としないことによって）ことができる。

【００５８】

図６は、安全な第三者データ記憶のための例示的なシステム６００を例解する。図６に示されるように、例示的なシステム６００は、第三者記憶サーバ６２０によって容易にされた第三者記憶サービスを介して１つ以上のファイルを記憶し、及び／又はそれにアクセスするように構成されるクライアントシステム６１０（１）及び６１０（２）を含むことができる。例えば、第三者記憶サーバ６２０は、クライアントシステム６１０（１）の代わりに暗号化ファイル６４０、６４２、及び６４４を記憶することができる。この例では、非対称キーペア６３０（１）は、クライアントシステム６１０（１）に対応することができ、非対称キーペア６３０（２）は、クライアントシステム６１０（２）に対応することができる。したがって、暗号化ファイル６４０、６４２、及び６４４は、暗号化されたファイルキー６４１、６４３、及び６４５でそれぞれ暗号化されてもよく、同様に暗号化キー６３２（１）で暗号化されてもよい。

【００５９】

工程６５０では、クライアントシステム６１０（１）は、暗号化ファイル６４０、６４２、及び６４４の暗号化されていないコンテンツへのアクセスをクライアントシステム６１０（２）と共有する要求を第三者記憶サーバ６２０に送信することができる。この要求は、クライアント側キー６１２（１）を含むことができる。第三者記憶サーバ６２０は、クライアント側キー６１２（１）を受信し、工程６５２で、暗号化された復号キー６３４（１）をクライアント側キー６１２（１）で復号して、復号キー６３６（１）を得ることができる。

【００６０】

工程６５４では、第三者記憶サーバ６２０は、復号キー６３６（１）を暗号化キー６３２（２）で暗号化して、暗号化された復号キー６３８を得ることができる。第三者記憶サーバ６２０は次に、将来の使用のために暗号化された復号キー６３８を記憶することができる。その後、工程６５６では、クライアントシステム６１０（２）は、暗号化ファイル６４０、６４２、及び６４４のうちの１つ以上にアクセスするクライアント側キー６１２（２）を含む要求を第三者記憶サーバ６２０に送信することができる。第三者記憶サーバ６２０は次に、暗号化された復号キー６３８を暗号化された復号キー６３４（２）で復号して復号キー６３６（１）を得て、かつ暗号化されたファイルキー６４１、６４３、及び６４５のうちの１つ以上を復号キー６３６（１）で復号して、暗号化ファイル６４０、６４２、及び６４４のうちの１つ以上の暗号化されていないコンテンツを得ることによってアクセスを提供することができる。

【００６１】

図３の工程３１０に戻り、いくつかの例では、アクセスモジュール１１２は、ユーザアカウントのグループの会員であることに基づいて暗号化ファイルの暗号化されていないバージョンへのアクセスを提供することができる。例えば、アクセスモジュール１１２は、ユーザアカウントを含むユーザアカウントのグループに指定された追加の非対称キーペアを識別することができる。追加の非対称キーペアは、追加の暗号化キーと、追加の復号キ

ーとを含むことができる。追加の復号キーは、ユーザアカウントの非対称キーペアに対応する暗号化キーで暗号化されてもよい。アクセスモジュール１１２は次に、追加の復号キーを復号キーで復号することができる。アクセスモジュール１１２は、暗号化ファイルを暗号化するために使用されるファイルキーを更に識別することができる。ファイルキーは、追加の暗号化キーで暗号化されてもよい。アクセスモジュール１１２は、ファイルキーを追加の復号キーで復号し、暗号化ファイルをファイルキーで復号することができる。更なる例では、アクセスモジュール１１２は、ファイルキーの代わりに追加の暗号化キーで暗号化されてもよい。この例では、アクセスモジュール１１２は、暗号化ファイルを追加の復号キーで単純に復号することができる。

【００６２】

図７は、安全な第三者データ記憶のための例示的なシステム７００を例解する。図７に示されるように、例示的なシステム７００は、第三者記憶サーバ７２０によって容易にされた第三者記憶サービスを介して１つ以上のファイルを記憶し、及び／又はそれにアクセスするように構成されるクライアントシステム７１０（１）、７１０（２）、及び７１０（３）を含むことができる。例えば、第三者記憶サーバ７２０は、クライアントシステム７１０（１）～（３）の代わりに暗号化ファイル７４６、７４７、及び７４８を記憶することができる。この例では、パーソナル非対称キーペア７３０（１）は、クライアントシステム７１０（１）に対応することができ、グループ非対称キーペア７４０（２）は、グループ（例えば、各々が暗号化された復号キー７４４（１）、７４４（２）、及び７４４（３）をそれぞれ持つ、グループ復号キー７３８の暗号化されたバージョンを有する、クライアントシステム７１０（１）、７１０（２）、及び７１０（３）で）としてクライアントシステム７１０（１）～（３）に対応することができる。暗号化ファイル７４６、７４７、及び７４８は、暗号化キー７４２で暗号化されてもよい。

【００６３】

工程７５０では、クライアントシステム７１０（１）は、暗号化ファイル７４０の暗号化されていないコンテンツにアクセスする要求を第三者記憶サーバ７２０に送信することができる。この要求は、クライアント側キー７１２（１）を含むことができる。第三者記憶サーバ７２０は、クライアント側キー７１２（１）を受信し、工程７５２では、暗号化された復号キー７３４（１）をクライアント側キー７１２（１）で復号して、パーソナル復号キー７３６（１）を得ることができる。工程７５４では、第三者記憶サーバ７２０は、暗号化された復号キー７４４（１）をパーソナル復号キー７３６（１）で復号して、グループ復号キー７３８を得ることができる。工程７５６では、第三者記憶サーバ７２０は、暗号化ファイル７４６をグループ復号キー７３８で復号して、暗号化されていないファイル７４９を得ることができる。工程７５８では、第三者記憶サーバ７２０は、暗号化されていないファイル７４９をクライアントシステム７１０（１）に送信することができる。同様の様式で、第三者記憶サーバ７２０は、暗号化された復号キー７４４（２）及び７４４（３）をクライアント側キー７１２（２）及び７１２（３）でそれぞれ復号することによって、クライアントシステム７１０（２）及び７１０（３）に対する暗号化ファイル７４６、７４７、及び／又は７４８の暗号化されていないバージョンを得ることができる。あるいは、前述のように、いくつかの例では、暗号化ファイル７４６、７４７、及び７４８は各々、それぞれのファイルキーで暗号化されてもよく、同様に、各々が暗号化キー７４２で暗号化されてもよい。これらの例では、第三者記憶サーバ７２０は、ファイルキーをグループ復号キー７３８で復号し、次いで暗号化ファイル７４６、７４７、及び７４８をそれぞれのファイルキーで復号することができる。

【００６４】

上記に説明されるように、安全化されたデータを暗号化及び復号するための非対称キーペアを第三者記憶サーバ上に維持し、非対称キーペアの復号キーをクライアントによって維持される暗号化キーで暗号化することによって、本明細書に記載されるシステム及び方法は、暗号化されていない状態で、安全化されたデータにアクセスするために必要なクライアント側復号キーを記憶することなく、クライアントデータを安全に記憶及び暗号化す

ることができる。それにより、これらのシステム及び方法は、この安全化されたデータの共有、重複排除、分析、及び／若しくは索引付けを更に可能にし、並びに／又は容易にしながら、第三者記憶システムへのアクセスを得た攻撃者が暗号化されていない状態の安全化されたデータにアクセスするのを防ぐことができる。

【００６５】

図８は、本明細書に記載及び／又は例解される実施形態のうちの１つ以上を実装することが可能な例示的なコンピューティングシステム８１０のブロック図である。例えば、コンピューティングシステム８１０の全て又は一部分は、単独又は他の要素との組み合わせのいずれかで、本明細書に記載される工程を識別すること、受信すること、生成すること、暗号化すること、重複排除すること、記憶すること、復号すること、使用すること、アクセスすること、送信すること、生成すること、実施すること、索引付けすること、及び提供することのうちの１つ以上を実施し得る、及び／又はそれを実施するための手段であり得る。コンピューティングシステム８１０の全て又は一部分はまた、本明細書に記載及び／又は例解される任意の他の工程、方法、又はプロセスを実施し得る、及び／又は実施するための手段であり得る。

【００６６】

コンピューティングシステム８１０は、コンピュータで読み取り可能な命令を実行することが可能な任意の単一又はマルチプロセッサコンピューティングデバイス又はシステムを広範に表す。コンピューティングシステム８１０の例としては、これらに限定されないが、ワークステーション、ラップトップ、クライアント側端末、サーバ、分散型コンピューティングシステム、ノートデバイス、又は任意の他のコンピューティングシステム又はデバイスが挙げられる。最も基本的な構成において、コンピューティングシステム８１０は、少なくとも１つのプロセッサ８１４及びシステムメモリ８１６を含み得る。

【００６７】

プロセッサ８１４は、概して、データ処理又は命令の解釈及び実行が可能な任意のタイプ又は形態の処理ユニットを表す。ある実施形態において、プロセッサ８１４は、ソフトウェアアプリケーション又はモジュールから命令を受信し得る。これらの命令は、プロセッサ８１４に、本明細書に記載及び／又は例解される例示的な実施形態のうちの１つ以上の機能を実施させ得る。

【００６８】

システムメモリ８１６は、概して、データ及び／又は他のコンピュータで読み取り可能な命令を記憶することが可能な揮発性又は非揮発性の記憶デバイス又は媒体の任意のタイプ又は形態を表す。システムメモリ８１６の例としては、これらに限定されないが、ランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、フラッシュメモリ、又は任意の他の好適なメモリデバイスが挙げられる。必ずしも必要ではないが、ある実施形態において、コンピューティングシステム８１０は、揮発性メモリユニット（例えば、システムメモリ８１６等）及び非揮発性記憶デバイス（例えば、以下に詳細に説明されるように、一次記憶デバイス８３２等）を含み得る。一実施例において、図１からのモジュール１０２のうちの１つ以上は、システムメモリ８１６にロードされ得る。

【００６９】

ある実施形態において、例示的なコンピューティングシステム８１０はまた、プロセッサ８１４及びシステムメモリ８１６に加えて、１つ以上の構成要素又は要素を含んでもよい。例えば、図８に例解されるように、コンピューティングシステム８１０は、通信基盤８１８を介して各々が相互接続され得る、メモリコントローラ８２０、入力／出力（Ｉ／Ｏ）コントローラ８２２、及び通信インターフェース８１２を含んでもよい。通信基盤８１２は、概して、コンピューティングデバイスの１つ以上の構成要素の間の通信を容易にすることが可能な任意のタイプ又は形態の基盤を表し得る。通信基盤８１２の例としては、これらに限定されないが、通信バス（ＩＳＡ、ＰＣＩ、ＰＣＩｅ、類似のバス等）及びネットワークが挙げられる。

【００７０】

メモリコントローラ８１８は、概して、コンピューティングシステム８１０の１つ以上の構成要素間でメモリ若しくはデータを扱う、又は通信を制御することが可能な任意のタイプ又は形態のデバイスを表し得る。例えば、ある実施形態において、メモリコントローラ８１８は、通信基盤８１２を介して、プロセッサ８１４、システムメモリ８１６、及びＩ／Ｏコントローラ８２０との間で通信を制御し得る。

【００７１】

Ｉ／Ｏコントローラ８２０は、概して、コンピューティングデバイスの入力及び出力機能を調整及び／又は制御することが可能な任意のタイプ又は形態のモジュールを表し得る。例えば、ある実施形態において、Ｉ／Ｏコントローラ８２０は、プロセッサ８１４、システムメモリ８１６、通信インターフェース８２２、ディスプレイアダプタ８２６、入力インターフェース８３０、及び記憶インターフェース８３４のような、コンピューティングシステム８１０の１つ以上の要素間のデータの転送を制御又は容易にし得る。

【００７２】

通信インターフェース８２２は、広範に、例示的なコンピューティングシステム８１０と１つ以上の追加のデバイスとの間の通信を容易にすることが可能な任意のタイプ若しくは形態の通信デバイス又はアダプタを表し得る。例えば、ある実施形態において、通信インターフェース８２２は、コンピューティングシステム８１０と、追加のコンピューティングシステムを含む私的又は公的なネットワークとの間の通信を容易にし得る。通信インターフェース８２２の例としては、これらに限定されないが、有線ネットワークインターフェース（ネットワークインターフェースカード等）、無線ネットワークインターフェース（無線ネットワークインターフェースカード等）、モデム、及び任意の他の好適なインターフェースが挙げられる。少なくとも１つの実施形態において、通信インターフェース８２２は、インターネット等の、ネットワークへの直接的なリンクを介して、リモートサーバへ直接的な接続を提供し得る。通信インターフェース８２２はまた、例えば、ローカルエリアネットワーク（イーサネットネットワーク（「イーサネット」は登録商標、以下同じ）等）、パーソナルエリアネットワーク、電話若しくはケーブルネットワーク、携帯電話接続、衛星データ接続、又は任意の他の好適な接続を通じて、間接的にかかる接続を提供してもよい。

【００７３】

ある実施形態において、通信インターフェース８２２はまた、外部バス又は通信チャンネルを介して、コンピューティングシステム８１０と、１つ以上の追加のネットワーク又は記憶デバイスとの間の通信を容易にするように構成されるホストアダプタを表し得る。ホストアダプタの例としては、これらに限定されないが、ＳＣＳＩホストアダプタ、ＵＳＢホストアダプタ、ＩＥＥＥ　１３９４ホストアダプタ、ＳＡＴＡ及びｅＳＡＴＡホストアダプタ、ＡＴＡ及びＰＡＴＡホストアダプタ、ファイバーチャンネルインターフェースアダプタ、イーサネットアダプタ等が挙げられる。通信インターフェース８２２はまた、コンピューティングシステム８１０が、分散型又はリモートコンピューティングに関与することを可能にし得る。例えば、通信インターフェース８２２は、実行のためにリモートデバイスから命令を受信するか、又はリモートデバイスへ命令を送信することができる。

【００７４】

図８に例解されるように、コンピューティングシステム８１０はまた、ディスプレイアダプタ８２６を介して通信基盤８１２に連結される少なくとも１つのディスプレイデバイス８２４を含んでもよい。ディスプレイデバイス８２４は、概して、ディスプレイアダプタ８２６によって転送される情報を視覚的に表示することが可能な任意のタイプ又は形態のデバイスを表し得る。同様に、ディスプレイアダプタ８２６は、概して、ディスプレイデバイス８１２上で表示するために、通信基盤８２４から（又は、当該分野で周知の、フレームバッファから）グラフィック、テキスト、及び他のデータを転送するように構成される任意のタイプ又は形態のデバイスを表す。

【００７５】

図８に例解されるように、例示的なコンピューティングシステム８１０はまた、入力イ

ンターフェース８３０を介して通信基盤８１２に連結される少なくとも１つの入力デバイス８２８を含んでもよい。入力デバイス８２８は、概して、例示的なコンピューティングシステム８１０に、コンピュータ又は人間のいずれかが生成した入力を提供することが可能な任意のタイプ又は形態の入力デバイスを表し得る。入力デバイス８２８の例としては、これらに限定されないが、キーボード、ポインティングデバイス、音声認識デバイス、又は任意の他の入力デバイスが挙げられる。

【００７６】

図８に例解されるように、例示的なコンピューティングシステム８１０はまた、記憶インターフェース８３４を介して通信基盤８１２に連結される一次記憶デバイス８３２及びバックアップ記憶デバイス８３３を含んでもよい。記憶デバイス８３２及び８３３は、概して、データ及び／又は他のコンピュータで読み取り可能な命令を記憶することが可能な任意のタイプ又は形態の記憶デバイス又は媒体を表す。例えば、記憶デバイス８３２及び８３３は、磁気ディスクドライブ（例えば、いわゆるハードドライブ）、ソリッドステートドライブ、フロッピーディスクドライブ（「フロッピー」は登録商標、以下同じ）、磁気タイプドライブ、光ディスクドライブ、フラッシュドライブ等であり得る。記憶インターフェース８３４は、概して、記憶デバイス８３２及び８３３とコンピューティングシステム８１０の他の構成要素との間でデータを転送するための任意のタイプ又は形態のインターフェース又はデバイスを表す。

【００７７】

ある実施形態において、記憶デバイス８３２及び８３３は、コンピュータソフトウェア、データ、又は他のコンピュータで読み取り可能な情報を記憶するように構成される取り外し可能な記憶ユニットから読み取る、及び／又は取り外し可能な記憶ユニットに書き込むように構成されてもよい。好適な取り外し可能な記憶ユニットの例としては、これらに限定されないが、フロッピーディスク、磁気テープ、光ディスク、フラッシュメモリデバイス等が挙げられる。記憶デバイス８３２及び８３３はまた、コンピュータソフトウェア、データ、又は他のコンピュータで読み取り可能な命令がコンピューティングシステム８１０にロードされることを可能にするための他の類似の構造又はデバイスを含んでもよい。例えば、記憶デバイス８３２及び８３３は、ソフトウェア、データ、又は他のコンピュータで読み取り可能な情報を読み取る及び書き込むように構成され得る。記憶デバイス８３２及び８３３はまた、コンピューティングシステム８１０の一部であってもよく、又は他のインターフェースシステムを通じてアクセスされる別個のデバイスであってもよい。

【００７８】

多くの他のデバイス又はサブシステムが、コンピューティングシステム８１０に接続され得る。反対に、本明細書に記載及び／又は例解される実施形態を実践するために、図８に例解される構成要素及びデバイスの全てが存在する必要はない。上で言及されるデバイス及びサブシステムはまた、図８に示されるものとは異なる方法で相互接続されてもよい。コンピューティングシステム８１０はまた、任意の数のソフトウェア、ファームウェア、及び／又はハードウェア構成を用いてもよい。例えば、本明細書に開示される例示的な実施形態のうちの１つ以上は、コンピュータで読み取り可能な記憶媒体上で、コンピュータプログラム（コンピュータソフトウェア、ソフトウェアアプリケーション、コンピュータで読み取り可能な命令、又はコンピュータ制御論理とも称される）としてコード化され得る。「コンピュータで読み取り可能な記憶媒体」という句は、概して、コンピュータで読み取り可能な命令を記憶又は担持することが可能な任意の形態のデバイス、キャリア、又は媒体を指す。コンピュータ読み取り可能な記憶媒体の例としては、これらに限定されないが、搬送波等の伝送型媒体、並びに磁気記憶媒体（例えば、ハードディスクドライブ及びフロッピーディスク）、光記憶媒体（例えば、ＣＤ－又はＤＶＤ－ＲＯＭ）、電子記憶媒体（例えば、ソリッドステートドライブ及びフラッシュメディア）、及び他の分散システム等の非一時的型媒体が挙げられる。

【００７９】

コンピュータプログラムを含むコンピュータで読み取り可能な記憶媒体は、コンピュー

ティングシステム８１０にロードされ得る。次いで、コンピュータで読み取り可能な記憶媒体上に記憶されるコンピュータプログラムの全ての又は一部分は、システムメモリ８１６、並びに／又は記憶デバイス８３２及び８３３の多様な部分に記憶され得る。プロセッサ８１４により実行されるとき、コンピューティングシステム８１０にロードされるコンピュータプログラムは、プロセッサ８１４に、本明細書に記載及び／又は例解される例示的な実施形態のうちの１つ以上の機能を実施させ得る、及び／又は実施するための手段であり得る。更に又は代替的に、本明細書に記載及び／又は例解される例示的な実施形態のうちの１つ以上は、ファームウェア及び／又はハードウェアに実装され得る。例えば、コンピューティングシステム８１０は、本明細書に開示される例示的な実施形態のうちの１つ以上を実装するように適合される、特定用途向け集積回路（ＡＳＩＣ）として構成されてもよい。

【００８０】

図９は、クライアントシステム９１０、９２０、及び９３０、並びにサーバ９４０及び９４５がネットワーク９５０に連結され得る、例示的なネットワークアーキテクチャ９００のブロック図である。上記に詳述されるように、ネットワークアーキテクチャ９００の全て又は一部分は、単独又は他の要素との組み合わせのいずれかで、本明細書に開示される工程を識別すること、受信すること、生成すること、暗号化すること、重複排除すること、記憶すること、復号すること、使用すること、アクセスすること、送信すること、生成すること、実施すること、索引付けすること、及び提供することのうちの１つ以上を実施し得る、及び／又はそれを実施するための手段であり得る。ネットワークアーキテクチャ９００の全て又は一部分はまた、本開示に記載される他の工程及び特性を実施するために使用され得る、及び／又は実施するための手段であり得る。

【００８１】

クライアントシステム９１０、９２０、及び９３０は、概して、図８の例示的なコンピューティングシステム８１０等の、コンピューティングデバイス又はシステムの任意のタイプ又は形態を表し得る。同様に、サーバ９４０及び９４５は、概して、多様なデータベースサービスを提供する及び／又はあるソフトウェアアプリケーションを作動させるように構成される、アプリケーションサーバ又はデータベースサーバ等のコンピューティングデバイス又はシステムを表す。ネットワーク９５０は、概して、例えば、イントラネット、広域ネットワーク（ＷＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、パーソナルエリアネットワーク（ＰＡＮ）、又はインターネットを含む、任意の電気通信又はコンピュータネットワークを表す。一実施例において、クライアントシステム９１０、９２０、及び／若しくは９３０、並びに／又はサーバ９４０及び／若しくは９４５は、図１からのシステム１００の全ての又は一部分を含んでもよい。

【００８２】

図９に例解されるように、１つ以上の記憶デバイス９６０（１）～（Ｎ）は、サーバ９４０に直接接続され得る。同様に、１つ以上の記憶デバイス９７０（１）～（Ｎ）は、サーバ９４５に直接接続され得る。記憶デバイス９６０（１）～（Ｎ）及び記憶デバイス９７０（１）～（Ｎ）は、概して、データ及び／又は他のコンピュータで読み取り可能な命令を記憶することが可能な任意のタイプ又は形態の記憶デバイス又は媒体を表す。ある実施形態において、記憶デバイス９６０（１）～（Ｎ）及び記憶デバイス９７０（１）～（Ｎ）は、ＮＦＳ、ＳＭＢ、又はＣＩＦＳ等の、多様なプロトコルを使用してサーバ９４０及び９４５と通信するように構成されるネットワーク接続記憶（ＮＡＳ）デバイスを表し得る。

【００８３】

サーバ９４０及び９４５はまた、記憶エリアネットワーク（ＳＡＮ）ファブリック９８０に接続され得る。ＳＡＮファブリック９８０は、概して、複数の記憶デバイス間の通信を容易にすることが可能な任意のタイプ又は形態のコンピュータネットワーク又はアーキテクチャを表す。ＳＡＮファブリック９８０は、サーバ９４０及び９４５と複数の記憶デバイス９９０（１）～（Ｎ）及び／又は知的記憶アレイ９９５との間の通信を容易にし得

る。ＳＡＮファブリック９８０はまた、デバイス９９０（１）～（Ｎ）及びアレイ９９５が、クライアントシステム９１０、９２０、及び９３０にローカルで接続されたデバイスとして現れるような様式で、ネットワーク９５０並びにサーバ９４０及び９４５を介して、クライアントシステム９１０、９２０、及び９３０と記憶デバイス９９０（１）～（Ｎ）及び／又は知的記憶アレイ９９５との間の通信を容易にし得る。記憶デバイス９６０（１）～（Ｎ）及び記憶デバイス９７０（１）～（Ｎ）と同様に、記憶デバイス９９０（１）～（Ｎ）及び知的記憶アレイ９９５は、概して、データ及び／又は他のコンピュータで読み取り可能な命令を記憶することが可能な任意のタイプ又は形態の記憶デバイス又は媒体を表す。

【００８４】

ある実施形態において、及び図８の例示的なコンピューティングシステム８１０を参照して、図８の通信インターフェース８２２等の通信インターフェースは、各クライアントシステム９１０、９２０、及び９３０とネットワーク９５０との間の接続性を提供するために使用されてもよい。クライアントシステム９１０、９２０、及び９３０は、例えば、ウェブブラウザ又はその他のクライアントソフトウェアを使用して、サーバ９４０又は９４５上の情報にアクセスすることが可能であり得る。そのようなソフトウェアは、クライアントシステム９１０、９２０、及び９３０が、サーバ９４０、サーバ９４５、記憶デバイス９６０（１）～（Ｎ）、記憶デバイス９７０（１）～（Ｎ）、記憶デバイス９９０（１）～（Ｎ）、又は知的記憶アレイ９９５によりホストされるデータにアクセスすることを可能にし得る。図９は、データを交換するためのネットワーク（インターネット等）の使用を描写するが、本明細書に記載及び／又は例解される実施形態は、インターネット又はいかなる特定のネットワークに基づく環境にも限定されない。

【００８５】

少なくとも１つの実施形態において、本明細書に開示される例示的な実施形態のうちの１つ以上の全て又は一部分は、コンピュータプログラムとしてコード化され、サーバ９４０、サーバ９４５、記憶デバイス９６０（１）～（Ｎ）、記憶デバイス９７０（１）～（Ｎ）、記憶デバイス９９０（１）～（Ｎ）、知的記憶アレイ９９５、又はそれらの任意の組み合わせ上にロードされ、それによって実行され得る。本明細書に開示される少なくとも１つの例示的な実施形態の全て又は一部分は、コンピュータプログラムとしてとしてコード化され、サーバ９４０に記憶され、サーバ９４５により作動され、ネットワーク９５０を通じてクライアントシステム９１０、９２０、及び９３０に分散され得る。

【００８６】

上記に詳述されるように、コンピューティングシステム８１０及び／又はネットワークアーキテクチャ９００の１つ以上の構成要素は、単独又は他の要素との組み合わせのいずれかで、安全な第三者データ記憶のための例示的な方法の１つ以上の工程を実施し得る、及び／又はそれを実施するための手段であり得る。

【００８７】

先述の開示は、特定のブロック図、流れ図、及び実施例を使用して多様な実施形態を説明するが、本明細書に記載及び／又は例解される各ブロック図の構成要素、流れ図の工程、動作、及び／又は構成要素は、個別に及び／又は集合的に、広範なハードウェア、ソフトウェア、又はファームウェア（又はそれらの任意の組み合わせ）構成を使用して、実装されてもよい。更に、他の構成要素内に含まれる構成要素のいずれの開示も、多くの他のアーキテクチャが同じ機能性を達成するために実装することができるため、事実上例示的なものと見なされるべきである。

【００８８】

一部の実施例において、図１の例示的なシステム１００の全ての又は一部分は、クラウドコンピューティング又はネットワークに基づく環境の部分を表し得る。クラウドコンピューティング環境は、インターネットを介して多様なサービス及びアプリケーションを提供することができる。これらのクラウドに基づくサービス（例えば、サービスとしてのソフトウェア、サービスとしてのプラットフォーム、サービスとしての基盤等）は、ウェブ

ブラウザ又は他のリモートインターフェースを通じてアクセス可能であり得る。本明細書に記載の多様な機能は、リモートデスクトップ環境又は任意の他のクラウドに基づくコンピューティング環境を通じて提供され得る。

【００８９】

本明細書に記載及び／又は例解されるプロセスパラメータ及び工程の順序は、ほんの一例として提供され、所望に応じて変更することができる。例えば、本明細書に例解及び／又は記載される工程が特定の順序で示される又は論議されるが、これらの工程は、必ずしも例解又は論議される順序で実施される必要はない。本明細書に記載及び／又は例解される多様な例示的な方法はまた、本明細書に記載及び／又は例解される工程のうちの１つ以上を省略してもよく、又は開示されるものに加えて追加の工程を含んでもよい。

【００９０】

種々の実施形態が、完全に機能的なコンピューティングシステムの文脈において、本明細書に記載及び／又は例解されているが、これらの例示的な実施形態のうちの１つ以上は、実際に分散を行うために使用されるコンピュータで読み取り可能な記憶媒体の特定のタイプにかかわらず、多様な形態のプログラム製品として分散され得る。本明細書に開示の実施形態はまた、あるタスクを実施するソフトウェアモジュールを使用して実装されてもよい。これらのソフトウェアモジュールは、スクリプト、バッチ、又はコンピュータで読み取り可能な記憶媒体上又はコンピューティングシステムに記憶され得る、他の実行可能なファイルを含んでもよい。一部の実施例において、これらのソフトウェアモジュールは、本明細書に開示される例示的な実施形態のうちの１つ以上を実施するように、コンピューティングシステムを構成し得る。

【００９１】

更に、本明細書に記載のモジュールのうちの１つ以上は、データ、物理的デバイス、及び／又は物理的デバイスの表現を１つの形態から別の形態へ変換し得る。例えば、本明細書に列挙されるモジュールのうちの１つ以上は、コンピューティングデバイスを安全な第三者記憶のためのデバイスに変換することができる。別の例として、本明細書に列挙されるモジュールのうちの１つ以上は、暗号化ファイルを暗号化されていないファイルに変換することができる。

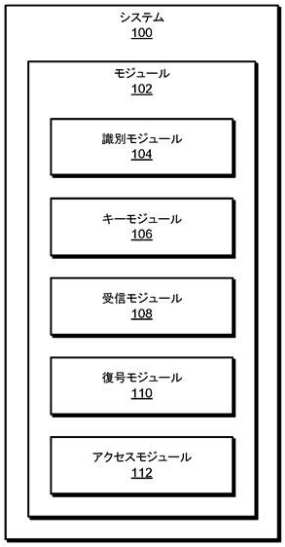
【００９２】

先行の説明は、他の当業者が、本明細書に開示される例示的な実施形態の多様な態様を最大限に利用することを可能にするように提供されている。この例示的な説明は、包括的であること、又は開示されるいずれの正確な形態にも限定されることを意図するものではない。多くの修正及び変形が、本開示の趣旨及び範囲から逸脱することなく可能である。本明細書に開示される実施形態は、あらゆる点で具体例であり、制限するものではないと見なされるべきである。本開示の範囲を決定する際、添付の特許請求の範囲及びその均等物への参照がなされるべきである。

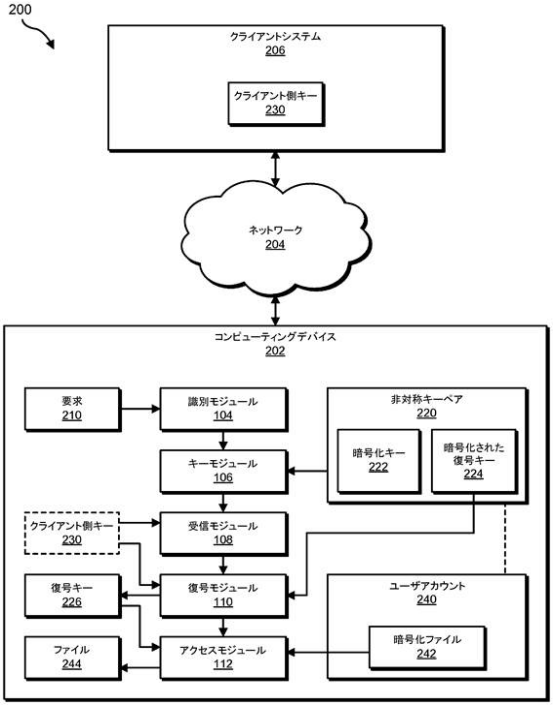
【００９３】

特に記されない限り、本明細書及び特許請求の範囲に使用される用語「ａ」又は「ａｎ」は、「少なくとも１つの」を意味すると解釈される。更に、使用の容易さのために、本明細書及び特許請求の範囲に使用される際、単語「含む」及び「有する」は、単語「備える」と同義であり、かつ同じ意味を有する。

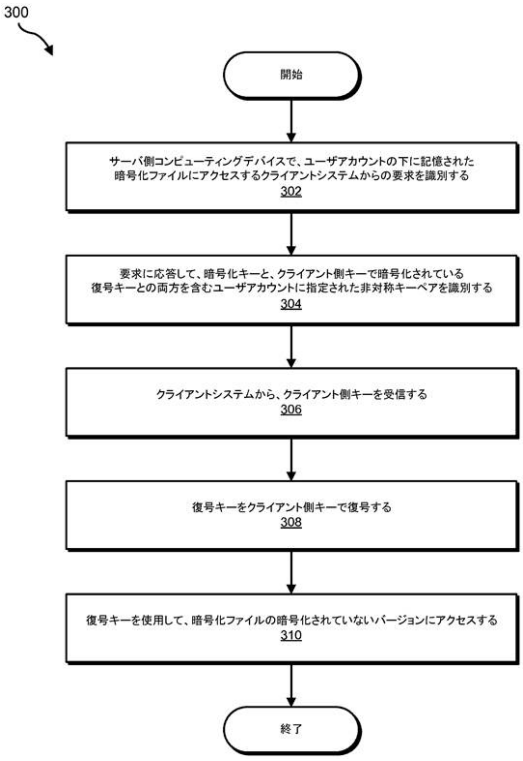
【図１】


システム
100
モジュール
102
識別モジュール
104
キーモジュール
106
受信モジュール
108
復号モジュール
110
アクセスモジュール
112

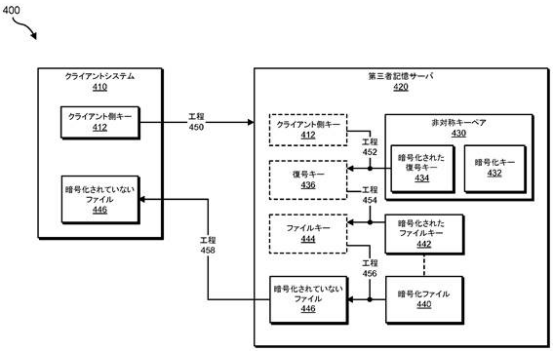
【図２】


200
クライアントシステム
206
クライアント側キー
230
ネットワーク
204
コンピューティングデバイス
202
要求
210
識別モジュール
104
非対称キーペア
220
暗号化キー
222
暗号化された
復号キー
224
キーモジュール
106
クライアント側キー
230
受信モジュール
108
復号キー
226
復号モジュール
110
ユーザアカウント
240
ファイル
244
アクセスモジュール
112
暗号化ファイル
242

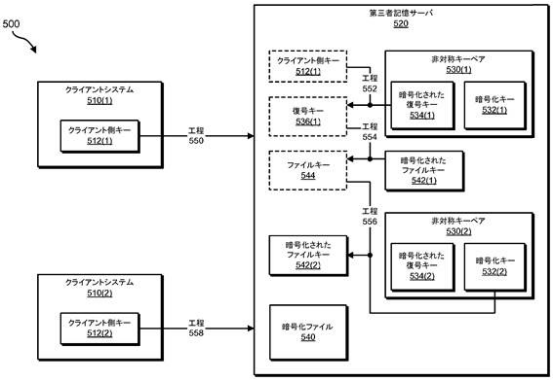
【図３】


300
開始
サーバ側コンピューティングデバイスで、ユーザアカウントの下に記憶された
暗号化ファイルにアクセスするクライアントシステムからの要求を識別する
302
要求に応答して、暗号化キーと、クライアント側キーで暗号化されている
復号キーとの両方を含むユーザアカウントに指定された非対称キーペアを識別する
304
クライアントシステムから、クライアント側キーを受信する
306
復号キーをクライアント側キーで復号する
308
復号キーを使用して、暗号化ファイルの暗号化されていないバージョンにアクセスする
310
終了

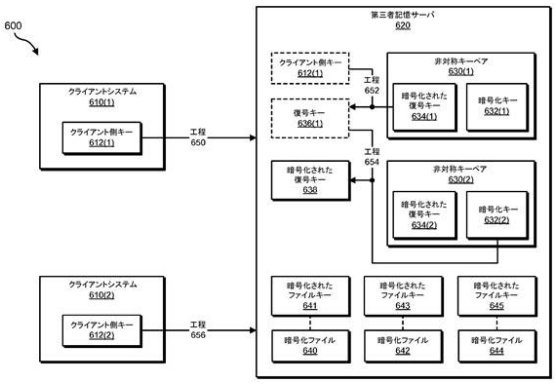
【図４】


400
クライアントシステム
410
クライアント側キー
412
暗号化されていない
ファイル
446
工程
450
工程
458
第三者記憶サーバ
420
クライアント側キー
412
非対称キーペア
430
暗号化された
復号キー
434
暗号化キー
432
復号キー
436
ファイルキー
444
暗号化された
ファイルキー
442
暗号化されていない
ファイル
446
暗号化ファイル
440
工程
452
工程
454
工程
456

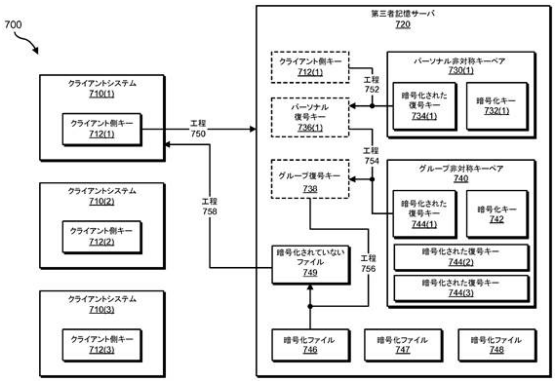
【図５】


500
クライアントシステム
510(1)
クライアント側キー
512(1)
工程
550
クライアントシステム
510(2)
クライアント側キー
512(2)
工程
558
第三者記憶サーバ
520
クライアント側キー
512(1)
非対称キーペア
530(1)
暗号化された
復号キー
534(1)
暗号化キー
532(1)
復号キー
536(1)
ファイルキー
544
暗号化された
ファイルキー
542(1)
暗号化された
ファイルキー
542(2)
非対称キーペア
530(2)
暗号化された
復号キー
534(2)
暗号化キー
532(2)
暗号化ファイル
540
工程
552
工程
554
工程
556

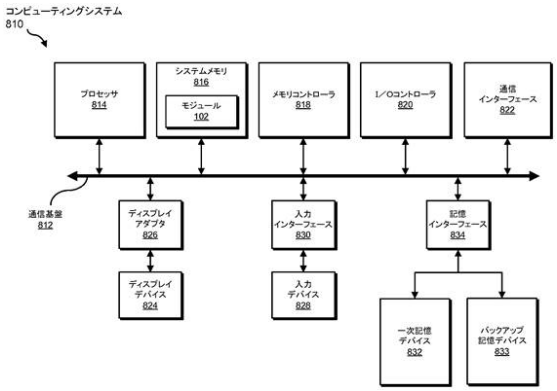
【図６】


600
第三者記憶サーバ
620
クライアントシステム
610(1)
クライアント側キー
612(1)
工程
650
クライアント側キー
612(1)
復号キー
636(1)
工程
652
非対称キーペア
630(1)
暗号化された
復号キー
634(1)
暗号化キー
632(1)
工程
654
暗号化された
復号キー
638
非対称キーペア
630(2)
暗号化された
復号キー
634(2)
暗号化キー
632(2)
クライアントシステム
610(2)
クライアント側キー
612(2)
工程
656
暗号化された
ファイルキー
641
暗号化された
ファイルキー
643
暗号化された
ファイルキー
645
暗号化ファイル
640
暗号化ファイル
642
暗号化ファイル
644

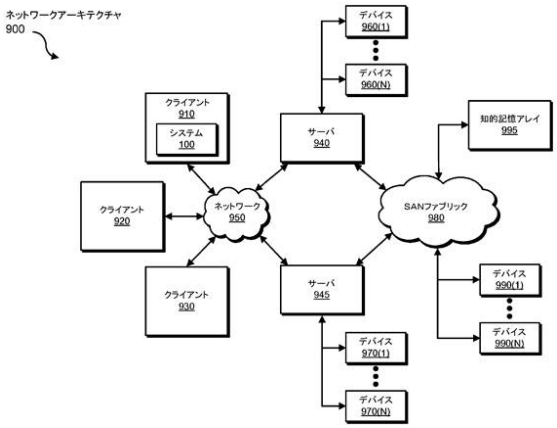
【図７】


700
第三者記憶サーバ
720
クライアントシステム
710(1)
クライアント側キー
712(1)
工程
750
クライアント側キー
712(1)
パーソナル
復号キー
736(1)
工程
752
パーソナル非対称キーペア
730(1)
暗号化された
復号キー
734(1)
暗号化キー
732(1)
クライアントシステム
710(2)
クライアント側キー
712(2)
工程
754
グループ復号キー
738
グループ非対称キーペア
740
暗号化された
復号キー
744(1)
暗号化キー
742
工程
758
暗号化されていない
ファイル
749
工程
756
暗号化された復号キー
744(2)
暗号化された復号キー
744(3)
クライアントシステム
710(3)
クライアント側キー
712(3)
暗号化ファイル
746
暗号化ファイル
747
暗号化ファイル
748

【図８】


コンピューティングシステム
810
プロセッサ
814
システムメモリ
816
モジュール
102
メモリコントローラ
818
I/Oコントローラ
820
通信
インターフェース
822
通信基盤
812
ディスプレイ
アダプタ
826
入力
インターフェース
830
記憶
インターフェース
834
ディスプレイ
デバイス
824
入力
デバイス
828
一次記憶
デバイス
832
バックアップ
記憶デバイス
833

【図９】


ネットワークアーキテクチャ
900
デバイス
960(1)
デバイス
960(N)
クライアント
910
システム
100
サーバ
940
知的記憶アレイ
995
クライアント
920
ネットワーク
950
SANファブリック
980
クライアント
930
サーバ
945
デバイス
990(1)
デバイス
990(N)
デバイス
970(1)
デバイス
970(N)

フロントページの続き

(56)参考文献 米国特許出願公開第２０１１／０１５４０３１（ＵＳ，Ａ１）
特開２００６－３４５２６１（ＪＰ，Ａ）
特表２００７－５３１１２７（ＪＰ，Ａ）
特開２０００－０１１００１（ＪＰ，Ａ）
特開２００５－１９０１３５（ＪＰ，Ａ）
特開２０１０－０９７５５０（ＪＰ，Ａ）
特開２０００－１７２５４８（ＪＰ，Ａ）
国際公開第２０１１／０１８８５２（WO，Ａ１）
特開２００２－３１４５２７（ＪＰ，Ａ）
特表２０１３－５１５３８５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　１２／００
Ｇ０６Ｆ　２１／６０
Ｈ０４Ｌ　９／０８