(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6854529号
(P6854529)
(45)発行日　令和3年4月7日(2021.4.7)　(24)登録日　令和3年3月18日(2021.3.18)

(51)Int.Cl.　　F I
H04L 9/10 (2006.01)　　H04L 9/00 621A
G06F 21/60 (2013.01)　　G06F 21/60 320

請求項の数 20　(全 22 頁)

(21)出願番号　特願2018-533811(P2018-533811)
(86)(22)出願日　平成29年1月3日(2017.1.3)
(65)公表番号　特表2019-501592(P2019-501592A)
(43)公表日　平成31年1月17日(2019.1.17)
(86)国際出願番号　PCT/AU2017/000002
(87)国際公開番号　WO2017/106938
(87)国際公開日　平成29年6月29日(2017.6.29)
審査請求日　令和1年12月18日(2019.12.18)
(31)優先権主張番号　2015905400
(32)優先日　平成27年12月24日(2015.12.24)
(33)優先権主張国・地域又は機関
オーストラリア(AU)

(73)特許権者　518220523
ヘヴンテック　プロプライエタリー　リミテッド
Ｈａｖｅｎｔｅｃ　Ｐｔｙ　Ｌｔｄ
オーストラリア連邦　ニューサウスウェールズ州　２０００，シドニー，マーケットストリート　１，レベル　２７
(74)代理人　110001302
特許業務法人北青山インターナショナル
(72)発明者　リチャードソン，リック　ビー．
オーストラリア連邦　ニューサウスウェールズ州　２４８１，サフォークパーク，アルコンストリート　１

審査官　行田　悦資

最終頁に続く

(54)【発明の名称】改良型ストレージシステム

(57)【特許請求の範囲】
【請求項１】
クライアントサーバ環境において、第２の位置で使用するデータをセキュアに保存する方法であって、
ユーザによる、前記第２の位置の前記データをセキュアに保存する方法の第１の使用のために、
前記ユーザが、サーバの形態の第１の装置へのセキュアな接続を開始するステップと、
第２の位置の前記ユーザのクライアント装置が、セキュアなユーザアカウントにログオンするステップと、
続いて、前記第１の位置の前記サーバが、前記ユーザに使用されるフォームを供給して、保護すべき前記データ要素をフォーマットするステップと、
前記ユーザが、保護すべき前記データ要素を前記フォームに入力するステップと、
その後、前記ユーザが、前記第２の位置の自分のクライアント装置に前記データ要素をセキュアに保存することを選択するステップと、
その後、前記第１の位置の前記サーバが、前記データ要素を前記第２の位置から取り込んで、処理するステップと、
続いて、暗号鍵が、前記第１の位置の前記サーバにより生成され、前記鍵が、前記セキュアなユーザアカウントにリンクされるステップと、
その後、前記鍵が、保護すべき前記データ要素を暗号化するために使用され、それに

より得られた暗号化データ要素が、前記第２の位置の前記ユーザのクライアント装置に保存されるステップと、を実行すること、並びに、
前記方法の第２の使用のために、
前記ユーザがセキュアな接続を開始した後、前記サーバが、前記セキュアなユーザアカウントを用いてセキュアな接続を確立するステップと、
第２の使用の過程において、前記第１の位置の前記サーバが前記ユーザにフォームを示して、前記暗号化データ要素であって、前記ユーザが過去に暗号化して前記第２の位置のクライアント装置にセキュアに保存することを選択した前記暗号化データ要素を収集するステップと、
その後、前記ユーザに選択肢が与えられ、前記ユーザが、前記第２の位置の前記クライアント装置に既に保存された前記暗号化データ要素を使用することを選択するステップと、
前記第１の位置の前記サーバが、前記第２の位置の前記クライアント装置から前記暗号化データ要素を取り込むステップと、
その後、前記サーバが、関連するセキュアなユーザアカウントから復号鍵を取り出し、前記データ要素が、前記サーバ上でメモリに復号されて、前記ユーザに利用可能となり、必要に応じて前記データが処理されるステップと、
続いて、前記ユーザによる前記データ要素の使用後に、前記サーバが、前記データ要素を前記第２の位置の前記クライアント装置に再び保存できるように、前記データ要素を再暗号化するのに用いられる新たな暗号鍵を生成するステップと、
その後、前記新たな暗号鍵が、将来の復号化及び使用に備えて、前記第１の位置の前記サーバに、前記セキュアなユーザアカウントと共に保存されるステップと、
その後、前記サーバが、前記サーバ上の前記データ及び前記暗号化データの全てを削除し、前記新たな暗号鍵が、前記サーバのみに保存されたままとするステップと、を実行すること、
を含むことを特徴とする方法。
【請求項２】
請求項１に記載の方法において、前記データ要素は、前記第２の位置で生成されることを特徴とする方法。
【請求項３】
請求項１又は２に記載の方法において、前記第２のステップにおいて、前記データ要素は、前記第２の位置の前記クライアント装置で用いられることを特徴とする方法。
【請求項４】
請求項１、２、又は３に記載の方法において、前記クライアント装置は、将来取り出せるように、前記暗号化データ要素を、ブラウザ又はＷｅｂ対応アプリケーションのローカルストレージに保存することを特徴とする方法。
【請求項５】
請求項１、又は２、又は３に記載の方法において、前記第１の位置は、Ｗｅｂ対応アプリケーションとして構成されることを特徴とする方法。
【請求項６】
請求項１乃至５のいずれか一項に記載の方法において、使用後の前記データ要素の暗号化ステップは、新たな暗号鍵を生成するステップを含むことを特徴とする方法。
【請求項７】
請求項１乃至６のいずれか一項に記載の方法において、前記データ要素は、使用中に修正されることを特徴とする方法。
【請求項８】
請求項１乃至７のいずれか一項に記載の方法において、前記データ要素は、前記ユーザに対して認証されることを特徴とする方法。
【請求項９】
請求項１乃至８のいずれか一項に記載の方法において、前記暗号化データ要素に対する

復号鍵は、前記第１の位置で生成され、前記第１の位置又はそのネットワーク環境内に保存されることを特徴とする方法。
【請求項１０】
請求項１乃至９のいずれか一項に記載の方法において、前記第１の位置は、サーバ装置により構成され、前記鍵は、前記サーバ装置又はそのネットワーク環境内に保存されることを特徴とする方法。
【請求項１１】
請求項１乃至１０のいずれか一項に記載の方法において、前記クライアント装置は、ストレージ機能を有するＷｅｂ対応アプリケーションを実行するようプログラムされることを特徴とする方法。
【請求項１２】
請求項１乃至１１のいずれか一項に記載の方法において、前記暗号化データ要素は、前記Ｗｅｂ対応アプリケーションのストレージ機能を用いて、前記クライアント装置に保存されることを特徴とする方法。
【請求項１３】
請求項１１に記載の方法において、前記Ｗｅｂ対応アプリケーションは、Ｗｅｂブラウザであることを特徴とする方法。
【請求項１４】
請求項１３に記載の方法において、前記Ｗｅｂブラウザは、ＨＴＭＬ５ローカルストレージ機能を含むＨＴＭＬ５を実行することを特徴とする方法。
【請求項１５】
クライアントサーバ環境において、データをセキュアに保存するための方法であって、前記データがユーザネームアカウントに対して参照されるものであり、
前記方法が、第１の位置に配置されたプロセッサを用いて、前記データを前記第１の位置で暗号化するステップであって、そのようにして暗号化されたデータが暗号化データを含み、前記暗号化データが、当該暗号化データを復号する鍵を必要とする、ステップと、
前記クライアント装置のためのユーザネームアカウントに対して参照される復号鍵を前記第１の位置で保存するステップであって、前記鍵が、前記第１の位置又はそのネットワーク環境内に保存される、ステップと、
前記暗号化データが、前記第１の位置から離れた第２の位置に送信されて、データに更なる処理を行うことが必要とされるときまで、前記第２の位置で保存され、データに更なる処理を行うことが必要とされる時点で、暗号化されていないウィンドウ期間中に復号されたデータを使用するために、前記暗号化データが前記第１の位置に送信されて、前記プロセッサにより実行される復号アルゴリズムに前記鍵を適用することにより、暗号化されていない状態とされるステップと、
前記暗号化されていないウィンドウ期間の終わりに、前記第１の位置の前記プロセッサが前記データを再暗号化して、再暗号化データを形成するステップと、
前記再暗号化データを前記クライアント装置に保存するステップと、
その後、前記第１の位置の前記プロセッサ上の前記データ及び前記暗号化データの全てを削除して、前記暗号化されていないウィンドウ期間を終了するステップであって、復号鍵が、前記第１の位置のプロセッサのみに保存されたままとする、ステップと、
を具えることを特徴とする方法。
【請求項１６】
クライアントサーバ環境における、データのセキュアストレージのための装置であって、
前記装置が、鍵を用いてデータを暗号化する第１のプロセッサを第１の位置に具え、前記装置が更に、前記第１の位置から離れた第２の位置に配置された第２のプロセッサを具え、
前記データは、暗号化後、ネットワークを介して前記第２のプロセッサに移動されて、前記第１のプロセッサ上のアプリケーションの実行に当該データが必要とされるときまで

、前記第２のプロセッサに関連して保存され、前記第１のプロセッサ上のアプリケーションの実行に当該データが必要とされる時点で、当該データは、前記第２のプロセッサから前記第１のプロセッサに戻されて、前記第１のプロセッサが、前記第１のプロセッサ上で実行するアプリケーションによる使用のために、復号化アルゴリズムに前記鍵を適用して前記データを復号し、復号したデータを暗号化されていないウィンドウ期間中に使用するために、前記データが、暗号化されていないウィンドウ期間中に、前記第２の位置でアクセス可能となり、

前記暗号化されていないウィンドウ期間の終わりに、前記第１の位置の前記第１のプロセッサが、前記データを再暗号化して、再暗号化データを形成し、前記再暗号化データを前記第２の位置の前記第２のプロセッサに保存し、その後、前記第１の位置の前記第１のプロセッサ上の前記データ及び前記暗号化データの全てを削除して、前記暗号化されていないウィンドウ期間を終了し、復号鍵が、前記第１の位置の前記第１のプロセッサのみに保存されたままとすることを特徴とする装置。

【請求項１７】

鍵により暗号化されたデータを前記鍵から分離する方法であって、前記データの復号化のためにユーザによる前記鍵の別個の取り出しを不要とする方法において、

クライアント／サーバ環境において、サーバが、前記鍵をユーザと関連付けるステップと、

ユーザによる認証により、ユーザにより操作されるクライアントが、暗号化されていないウィンドウ期間中に、データを前記サーバから受信するステップと、

ユーザが、前記暗号化されていないウィンドウ期間中に、前記クライアントにおいて前記データを使用するステップと、

ユーザによる認証により、前記クライアントが、前記暗号化されていないウィンドウ期間の終わりに、前記データを前記サーバに送信するステップと、

前記サーバが、前記鍵を参照して前記データを暗号化して、暗号化データを形成するステップと、

その後、前記サーバが、前記暗号化データを前記クライアントに送信するステップと、

その後、前記サーバが、前記サーバ上の前記データ及び前記暗号化データの全てを削除して、前記暗号化されていないウィンドウ期間を終了するステップとを具え、

前記鍵が、前記サーバのみに保存されたままとすることを特徴とする方法。

【請求項１８】

クライアント装置に保存された暗号化データをその復号鍵から分離する方法であって、

クライアント装置のユーザネームアカウント／ユーザログインデータに対して参照される前記復号鍵を別個の装置に保存するステップと、

復号したデータを暗号化されていないウィンドウ期間中に使用するために、前記暗号化データを前記別個の装置に転送して、前記ユーザログイン／ユーザネームアカウントの認証時に、前記復号鍵を用いて前記暗号化データを復号することにより、データを取り出すステップと、

前記暗号化されていない期間の終わりに、前記別個の装置が前記データを再暗号化して、再暗号化データを形成するステップと、

前記再暗号化データを前記クライアント装置に保存するステップと、

その後、前記別個の装置における前記データ及び前記暗号化データの全てを削除して、前記暗号化されていない期間を終了するステップとを具え、

前記復号鍵が、前記別個の装置にのみ保存されたままとすることを特徴とする方法。

【請求項１９】

請求項１７又は１８に記載の方法において、前記別個の装置は、Ｗｅｂサーバであることを特徴とする方法。

【請求項２０】

請求項１７、又は１８、又は１９に記載の方法において、クライアントサーバ環境において、セキュアな不使用ウィンドウの間に、データは、前記暗号化データを復号する復号

化を要する暗号化データとして、前記クライアントにセキュアに保存され、前記復号鍵は、前記クライアントに保存されていないことを特徴とする方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、電子ネットワーク上のデータのストレージに関し、より詳細には、限定されるものではないが、電子ネットワーク経由でアクセス可能なデータのセキュアストレージに関する。

【背景技術】

【０００２】

集中サーバ上で極秘データ又はセキュアデータを保護することは、当技術分野において一般的に行われている。このことは、従来、サーバのセキュリティリソースが、同一のデータをクライアント側の装置に保存するよりも、より安全且つ効率的であると考えられていたため、データを保存するのに有効な方法であった。

【０００３】

しかし、より巧妙なハッキング攻撃の出現や、数多くの人々の大量の保存極秘データを一箇所に持つことに伴う固有の危険は、一箇所に集めて極秘データを保存することの技術的、法的、及び業務上の危険性が大きな負担になっていることを意味する。

【０００４】

反対に、暗号化データをクライアント側の装置に保存し、一方でリスク及び負担を分散させることは、典型的には、クライアント装置が復号鍵のストレージとしても用いられなければならないことや、復号鍵を携帯型の近くのソースから保存して取得する不便をユーザが被らなければならない点で、安全性の課題を提起している。セキュアなデータシステムにおいて、暗号化データ及び復号鍵を別々の安全なロケーションに保存することが必須であるが、それを実現するための現在の対策は、典型的には、ユーザにとって複雑且つ不便なものである。

【０００５】

Ｃｏｃｏｏｎ Ｄａｔａ Ｈｏｌｄｉｎｇｓ Ｌｉｍｉｔｅｄに譲渡されたＰＣＴ／ＡＵ２０１２／０００９４４［ＷＯ２０１３０２０１７８］［Ｎｕｓｓｂａｕｍ ｅｔ ａｌ］は、概して、ユーザレベル又はユーザ装置での暗号鍵又は復号鍵の管理の必要性をなくそうとする方法を開示している。この引用文献では、その管理機能が、別個のサーバ装置に移され、当該サーバ装置は、復号鍵が明らかになる前、又は復号鍵を使用する前に関係当事者の認証を利用する。第１９頁第４～１０行目の一部には、「更なる有利な点は、・・・足跡が残らないことであり、ソフトウェア又はセキュアなデータは、エグゼクティブ（すなわちクライアント）コンピュータにインストール又は維持されていない。」（下線部の文言を付加）とある。プロセスにより保護されたファイルをユーザ（クライアント）装置に保存するという教示は存在しない。

【０００６】

また、Ｅｄｕｃａｔｉｏｎａｌ Ｔｅｓｔｉｎｇ Ｓｅｒｖｉｃｅに譲渡されたＵＳ２００７／０１９８８２３［Ｂｌｅｗ ｅｔ ａｌ］（ＵＳ７５１９８１０も参照）も、エンドユーザを暗号化及び復号化の仕組みから隠すことを主要の課題とし、それには、エンドユーザが任意の暗号鍵又は復号鍵を認識せずに済むようにすることも含まれる。この引用文献では、暗号化及び復号化及びファイルの保護が、クライアント装置と明らかに離れたサーバ上で（複数のサーバ間のデータ転送を要する方法による好ましい形態で）実行されており、プロセスにより保護されたファイルをクライアント装置に保存するという教示はない。

【０００７】

開示された発明の実施形態は、これらの課題に対処するために設計される。

【０００８】

［注］

「具える（ｃｏｍｐｒｉｓｉｎｇ）」（及びその文法的な変化形）という用語は、本明細書においては、「のみからなる（ｃｏｎｓｉｓｔｉｎｇ　ｏｎｌｙ　ｏｆ）」という閉鎖的な意味ではなく、「有する（ｈａｖｉｎｇ）」又は「含む（ｉｎｃｌｕｄｉｎｇ）」という包括的な意味で用いられる。

【０００９】

本発明の技術背景における先行技術の上記説明は、その中で説明されたいずれかの情報が引用可能な先行技術であること、又は、任意の国の当業者の一般知識の一部であることを認めるものではない。

【発明の概要】

【００１０】

［定義］

クライアントサーバ環境：あるトポロジを有するコンピューティングリソースの配置であって、クライアント装置は、少なくとも論理的に、殆どの場合は通常物理的に離れたサーバ装置とネットワークを介して通信する。概して、サーバ装置は、通常クライアント装置よりも多くのリソースを有し、クライアント装置は、１又はそれ以上のサーバ装置との通信に少なくとも部分的に依拠して、クライアント装置上でタスクを実行する。

【００１１】

暗号化／復号化：データを含むファイルに関連して、アルゴリズムを適用し、それにより、逆アルゴリズムがデータに適用されて暗号化されていない形式に戻されない限り、データを実質的に解読できない形でデータが再フォーマットされることを伴う方法論である。好ましい形態において、「鍵」は、アルゴリズムの参照要素として用いられる。一部の形態では、データを復号化するものと同一の鍵を用いてデータを暗号化する。他の形態では、暗号化に用いられる鍵は、復号化に用いられる鍵と異なる。暗号化は、ファイル内のデータにアクセスするのにパスワードを要するが、ファイル内のデータそのものは再フォーマットされない単純なパスワード保護とは区別すべきである。

【００１２】

認証：本明細書における認証は、通常、エンティティに特有の、関連する、認証又は許可された機能の実行を可能にする前段として、そのエンティティの身元が所定の確信性レベルまで確認される方法論である。最も簡潔な形態では、認証は、ユーザネーム及びパスワードの組み合わせにより行われることが多く、すなわち、所定のユーザネームと対応パスワードのペアの提供が認証を構成する。エンティティは、特定のプラットフォームの個々のオペレーティングソフトウェアであるか、プラットフォームそのものであってよい。例として、スマートフォン等のクライアント装置は、エンティティとみなしてよい。スマートフォンの所定のユーザを、スマートフォンの代替のエンティティとしてみなしてよく、又はスマートフォンと同様エンティティとしてみなしてよい。

【００１３】

従って、本発明の１つの広い形態では、クライアントサーバ環境において、データをセキュアに保存する方法が提供され、当該方法は、

データ要素を第１の位置で生成するステップと、

データ要素を第１の位置で暗号化して、暗号化データ要素を形成するステップと、

暗号化データ要素を、第１の位置から離れている第２の位置に送信するステップと、

暗号化データ要素を第２の位置に保存するステップと、を具える。

【００１４】

本発明の更なる広い形態では、クライアントサーバ環境において、データをセキュアに保存する方法が提供され、当該方法は、

データ要素を第２の位置で生成するステップと、データ要素を第２の位置から離れた第１の位置に送信するステップと、

データ要素を第１の位置で暗号化して、暗号化データ要素を形成するステップと、

暗号化データ要素を、第１の位置から離れた第２の位置に送信するステップと、

暗号化データ要素を第２の位置に保存するステップと、を具え、第２の位置は、クライ

アント装置として構成される。
【００１５】
好ましくは、暗号化データ要素に対する復号鍵は、第１の位置に保存される。
【００１６】
好ましくは、第２の位置は、クライアント装置である。
【００１７】
好ましくは、クライアント装置は、ストレージ機能を有するＷｅｂ対応アプリケーションを実行するようプログラムされる。
【００１８】
好ましくは、暗号化データ要素は、Ｗｅｂ対応アプリケーションのストレージ機能を用いて、クライアント装置に保存される。
【００１９】
好ましくは、Ｗｅｂ対応アプリケーションは、Ｗｅｂブラウザである。
【００２０】
好ましくは、Ｗｅｂブラウザは、ＨＴＭＬ５ローカルストレージ機能を含むＨＴＭＬ５を実行する。
【００２１】
本発明の更なる広い形態では、クライアントサーバ環境において、データをセキュアに保存するための方法が提供され、当該方法は、第１の位置に配置されたプロセッサを用いて、データを第１の位置で暗号化するステップであって、そのようにして暗号化されたデータが暗号化データを含み、暗号化データが、当該暗号化データを復号する鍵を必要とし、鍵が、第１の位置に保存される、ステップと、暗号化データが、第１の位置から離れた第２の位置に送信されて、データに更なる処理を行うことが必要とされるときまで、第２の位置で保存され、データに更なる処理を行うことが必要とされる時点で、暗号化データが第１の位置に送信されて、プロセッサにより実行される復号アルゴリズムに鍵を適用することにより、暗号化されていない状態とされる、ステップと、を具える。
【００２２】
本発明の更なる広い形態では、クライアントサーバ環境における、データのセキュアストレージのための装置が提供され、装置が、鍵を用いてデータを暗号化する第１のプロセッサを第１の位置に具え、装置が更に、第１の位置から離れた第２の位置に配置された第２のプロセッサを具え、データは、暗号化後、ネットワークを介して第２のプロセッサに移動されて、第１のプロセッサ上のアプリケーションの実行に当該データが必要とされるときまで、第２のプロセッサに関連して保存され、第１のプロセッサ上のアプリケーションの実行に当該データが必要とされる時点で、当該データは、第２のプロセッサから第１のプロセッサに戻されて、第１のプロセッサが、第１のプロセッサ上で実行するアプリケーションによる使用のために、復号化アルゴリズムに鍵を適用してデータを復号する。
【００２３】
本発明の更なる広い形態では、鍵により暗号化されたデータを鍵から分離する方法であって、データの復号化のためにユーザによる鍵の別個の取り出しを不要とする方法において、当該方法は、クライアント／サーバ環境において、暗号化されていないウィンドウ期間中に、データをサーバから受信するステップと、暗号化されていないウィンドウ期間中に、クライアントにおいてデータを使用するステップと、暗号化されていないウィンドウ期間の終わりに、データをサーバに送信するステップと、サーバが、鍵を参照してデータを暗号化して、暗号化データを形成するステップと、その後、サーバが、暗号化データをクライアントに送信するステップと、その後、サーバが、サーバ上のデータ及び暗号化データの全てを削除して、暗号化されていないウィンドウ期間を終了するステップとを具え、鍵が、サーバのみに保存されたままとする。
【００２４】
本発明の更なる広い形態では、クライアント装置に保存された暗号化データをその復号鍵から分離する方法が提供され、当該方法は、クライアント装置のユーザネームアカウン

ト／ユーザログインデータに対して参照される復号鍵を別個の装置に保存するステップと、暗号化データを別個の装置に転送して、ユーザログイン／ユーザネームアカウントの認証時に、復号鍵を用いて暗号化データを復号することにより、データを取り出すステップとを具える。

【００２５】

好ましくは、別個の装置は、Ｗｅｂサーバである。

【００２６】

好ましくは、ユーザログインは、ユーザネーム及びパスワードである。

【００２７】

本発明の更なる広い形態では、クライアントサーバ環境において、セキュアな不使用ウィンドウが提供され、クライアントでセキュアに保存されているデータは、暗号化データを復号する復号化を要する暗号化データを有し、復号鍵は、クライアントに保存されていない。

【００２８】

好ましくは、復号鍵は、サーバに保存される。

【００２９】

好ましくは、暗号化／復号化は、クライアントで行われない。

【００３０】

好ましくは、暗号化／復号化は、サーバで行われる。

【００３１】

好ましくは、クライアント／サービスセッションの認証が有効な場合、又はクライアント／サービスセッションの認証が有効な場合のみ、復号鍵が使用のためにリリースされる。

【００３２】

好ましくは、環境は、ユーザレベルの認証を必要とする。

【００３３】

好ましくは、復号鍵は認証に対して参照される。

【００３４】

好ましくは、認証はユーザ装置レベルである。

【００３５】

好ましくは、データは少ないデータ量である。

【００３６】

好ましくは、データ量は１００ＭＢである。

【００３７】

好ましくは、データ量は５０ＭＢである。

【００３８】

好ましくは、データ量は１０ＭＢである。

【００３９】

好ましくは、データ量は１ＭＢである。

【００４０】

好ましくは、データ量は０．５ＭＢである。

【００４１】

好ましくは、データ量は０．１ＭＢである。

【００４２】

好ましくは、データは、増分的に変化するのみで、仮に変化してもユーザセッション毎である。

【００４３】

好ましくは、データの一部の要素のみが変化し、仮に変化してもユーザセッション毎である。

【００４４】

本発明の更なる広い形態では、データをセキュアに保存するための方法が提供され、当該方法は、データ要素を第１の位置で生成するステップと、データ要素を第１の位置で暗号化して、暗号化データ要素を形成するステップと、暗号化データ要素を、第１の位置から離れた第２の位置に送信するステップと、暗号化データ要素を第２の位置に保存するステップと、を具える。

【００４５】

好ましくは、暗号化データ要素に対する復号鍵は、第１の位置に保存される。

【００４６】

好ましくは、第２の位置は、クライアント装置である。

【００４７】

好ましくは、クライアント装置は、ストレージ機能を有するＷｅｂ対応アプリケーションを実行するようにプログラムされる。

【００４８】

好ましくは、Ｗｅｂ対応アプリケーションは、ＨＴＭＬ５ローカルストレージ機能を含むＨＴＭＬ５を実行する。

【００４９】

好ましくは、暗号化データ要素は、Ｗｅｂ対応アプリケーションのストレージ機能を用いてクライアント装置に保存される。

【００５０】

好ましくは、Ｗｅｂ対応アプリケーションは、Ｗｅｂブラウザである。

【００５１】

本発明の更なる広い形態では、データをセキュアに保存するための方法が提供され、当該方法は、第１の位置に配置されたプロセッサを用いて、データを第１の位置で暗号化するステップであって、そのようにして暗号化されたデータが暗号化データを含み、暗号化データが、当該暗号化データを復号する鍵を必要とし、鍵が、第１の位置に保存される、ステップと、暗号化データは、第１の位置から離れた第２の位置に送信されて、データに更に処理を行うことが必要とされるときまで、第２の位置に保存され、データに更に処理を行うことが必要とされる時点で、暗号化データが第１の位置に送信されて、プロセッサにより実行される復号アルゴリズムに鍵を適用することにより、暗号化されていない状態とされるステップと、を具える。

【００５２】

本発明の更なる広い形態では、データのセキュアストレージのための装置が提供され、当該装置が、鍵を用いてデータを暗号化する第１のプロセッサを第１の位置に具え、当該装置が更に、第１の位置から離れた第２の位置に配置された第２のプロセッサを具え、データは、暗号化後、ネットワークを介して第２のプロセッサに移動されて、第２のプロセッサに対応付けて保存され、第１のプロセッサ上のアプリケーションの実行にデータが必要とされるときまで、第２のプロセッサに関連して保存され、第１のプロセッサ上のアプリケーションの実行にデータが必要とされる時点で、データは、第２のプロセッサから第１のプロセッサに戻されて、第１のプロセッサが、第１のプロセッサで実行するアプリケーションによる使用のために、復号化アルゴリズムに鍵を適用してデータを復号する。

【図面の簡単な説明】

【００５３】

添付の図面を参照しながら、本発明の実施形態を説明する。

【００５４】

【図１】図１は、例示的な実施形態の主な構成要素である。

【００５５】

【図２】図２は、本発明の実施形態に係る、データの初期保存のための制御プロセスである。

【００５６】

【図３】図３は、本発明の実施形態に係る、暗号化データのその後の使用のための制御プ

ロセスである。
【００５７】
【図４】図４Ａ、４Ｂ、及び４Ｃは、本発明の例示的な実施形態の実行の一形態を図表で表す。
【００５８】
【図５】図５は、説明した実施形態のいずれかと用いるのに適したクライアント／サーバ環境をブロック図で示す。
【００５９】
【図６】図６Ａから６Ｐは、本発明の実施形態の実施例の実行ステップ、及び使用を示す。
【発明を実施するための形態】
【００６０】
図１は、例示的な実施形態の主な構成要素が記載されている。例示的な実施形態において、クライアント装置１０は、保存されるデータ１１の暗号化バージョンを保存する。データを復号する鍵１８はクライアント１０に保存されないが、通常はインターネット等のネットワーク１５を介してアクセス可能なサーバ１４に保存される。
【００６１】
データ１１を復号化する鍵１８は、サーバ１４へのセキュアなアクセスを有するユーザのデータベース１６における特定のユーザアカウント１７と関連付けて、サーバ１４に保存される。
【００６２】
暗号化データ１１は、クライアント装置１０で起動するブラウザ１２又はＷｅｂ対応アプリケーション１２のドメイン関連のローカルストレージエリア１３に保存される。
［ローカルストレージコードの例は、ｈｔｔｐ：／／ｗｗｗ．ｗ３ｓｃｈｏｏｌｓ．ｃｏｍ／ｈｔｍｌ／ｈｔｍｌ５＿ｗｅｂｓｔｏｒａｇｅ．ａｓｐで見ることができる。］
【００６３】
サーバ１４は、暗号化データファイル１１としてクライアント１０に後で保存されるデータの暗号化、収集、及び処理に関連する、又はそれらを伴う様々なプロセスに用いられる。
［暗号化は、ｈｔｔｐ：／／ｅｎ．ｗｉｋｉｐｅｄｉａ．ｏｒｇ／ｗｉｋｉ／Ａｄｖａｎｃｅｄ＿Ｅｎｃｒｙｐｔｉｏｎ＿Ｓｔａｎｄａｒｄで説明されているＡＥＳ暗号化アルゴリズムを含むことができる。］
【００６４】
図２には、データの初期保存及び暗号化のための制御プロセスが記載されている。ユーザ４０は、サーバ４１へのセキュアな接続を開始し（３０）、クライアント装置は、セキュアなユーザアカウントにログオンする（３１）。続いて、サーバ４０は、保護されるデータをフォーマットするためにユーザが使用するフォームを供給し（３２）、ユーザは、セキュアにすべきデータの一部又は全部をフォームに入力する（３３）。次に、ユーザは、クライアント装置でデータをセキュアに保存することを選択する（３４）。
【００６５】
その後、サーバは、入力データを取り込んで、それを処理する（３５）。処理は、データ検証及びインテグリティチェックを含んでも、含まなくてもよい。続いて、暗号鍵がサーバにより生成され（３６）、鍵が現在のユーザのアカウントとリンクされる（３７）。
【００６６】
その後、鍵は、保護すべきデータを暗号化するのに用いられ（３８）、それにより得られた１又は複数の暗号化データファイルは、後で取り出すことができるように、クライアント装置のブラウザ又はＷｅｂ対応アプリケーションのローカルストレージに保存される（３９）。
【００６７】
図３は、暗号化データのその後の使用のための制御プロセスを示す。最初に、ユーザが

セキュアな接続を開始した後（５０）、サーバがユーザアカウントを用いてセキュアな接続を確立する（５１）。

【００６８】

使用中に、サーバは、ユーザにフォームを示して、ユーザが過去に暗号化して自分の装置にセキュアに保存することを選択した情報を収集してもよい（５２）。次に、ユーザの選択肢が与えられ、ユーザは、クライアント装置に既に保存された暗号化データを用いることを選択する（５３）。

【００６９】

続いて、サーバは、クライアントローカルストレージより暗号化データを取り込む（５４）。その後、サーバは、関連付けられたユーザネームアカウントより復号鍵を取り出し（５５）、データは、サーバ上でメモリに復号され（５６）、データは必要に応じて処理される（５７）。

【００７０】

続いて、サーバは、データを再暗号化するために新たな暗号鍵を生成し（５９）、そのデータをクライアント装置ローカルストレージに再度セキュアに保存することができる（６０）。新たな暗号鍵は、将来の復号化及び使用に備えてユーザアカウントと共に保存される（６１）。

【００７１】

［例示的な実施形態］

図４Ａ、４Ｂ、及び４Ｃは、本発明の例示的な実施形態のトポロジ及び実行の一形態を図表で示す。

【００７２】

この場合、図４Ａを参照すると、ストレージシステム８０は、この例ではネットワーク８３を介してクライアント装置８２と通信するサーバ８１に依存している。この特定の例で、ネットワーク８３はインターネットを含み、それ自体はヘッダ８５で識別される宛先までパケットデータ８４を送信するように構成されたコンピュータの相互接続ネットワークを具える。多くの場合、クライアント装置８２は、携帯電話ネットワーク、又はｗｉｆｉ等の他の無線通信ネットワークを含む初期リンク８６によりネットワーク８３と電子通信を行うこととなる。

【００７３】

［セキュアではないウィンドウ期間］

この例では、クライアント装置８２は、クライアント装置メモリ８７及びクライアント装置プロセッサ８８を含み、メモリに保存されるコード８９は、プロセッサ８８により実行可能である。この場合、コード８９は、サーバ８１からコマンド９０及びデータ９１を受信するよう適合されたアプリケーションを含む。この場合、コマンド９０及びデータ９１は、フォーム構造９２内のフォームフィールドＦ１～Ｆ７の作成を可能にする。好ましい形態において、フォーム構造９２はサーバ８１で決定され、セキュアではないウィンドウ期間中にクライアント装置８２に送信されるコマンド９０及びデータ９１の一部を形成する。それぞれのフォームフィールドは、それぞれのデータＤ１～Ｄ７を受け入れることができ、それらのデータは、データ９１としてサーバ８１から受信されるか、或いはクライアント装置８２のローカルユーザにより挿入されるようにしてもよい。フォーム構造９２及びデータ９１は、ストレージシステム８０のセキュアではないウィンドウ期間中に、セキュアではないフォームで提示される。この期間中、データＤ１～Ｄ７がクライアント装置８２からサーバ８１に送信される。典型的にはクライアント装置８２から物理的に離れた場所に位置するサーバ８１は、セキュアなデータチャネル又はセキュアではないデータチャネルのいずれかを介してデータＤ１～Ｄ７を受信し、データＤ１～Ｄ７を、エンティティアカウント９４に対して参照されるサーバメモリ９３に保存する。

【００７４】

［セキュアなウィンドウ期間］

図４Ｂを参照すると、セキュアなウィンドウ期間は、サーバ８１が少なくとも１つの鍵

９５を参照してデータＤ１～Ｄ７を暗号化することにより暗号化データ９６を形成する時に始まり、その後、サーバ８１は、クライアント装置８２に対して、すなわちデータＤ１～Ｄ７を作成したクライアント装置であって、そこから、エンティティアカウント９４に対して参照されるサーバ８１に送信したクライアント装置８２に対して、暗号化データ９６を送信する。一つの形態において、エンティティアカウントは、クライアント装置８２自体により所有されてよい。別の形態において、エンティティアカウントは、データＤ１～Ｄ７を生成したクライアント装置８２で実行されるコード８９のユーザにより所有されてもよい。

【００７５】

いずれの場合でも、サーバ８１は、暗号化前と暗号化後の両方のデータを、エンティティアカウント９４に対して参照する。

【００７６】

好ましい形態において、サーバ８１はウェブサーバである。代替的な好ましい形態において、サーバは、クライアント装置８２でコード８９として実行するためのＡＰＩ等の形態のアプリケーションの機能を提供することができる。

【００７７】

データＤ１～Ｄ７が暗号化されてクライアント装置８２に送信されると、サーバ８１は、エンティティアカウント９４に対して保存された鍵９５のみを残して、データＤ１～Ｄ７の全てのインスタンスを、暗号化された形態であるか否かに関わらず、そのストレージから削除する。

【００７８】

このセキュアなウィンドウ期間中、クライアント装置８２は暗号化データ９６をクライアント装置メモリ８７にローカルに保存する。鍵９５はクライアント装置８２に提供されないことに留意されたい。

【００７９】

［データＤ１～Ｄ７のその後の使用］

図４Ｃを参照すると、クライアント装置８２での初期セッションに続くセッションとしてコード８９の実行を具えるセッションにおいて、セキュアではないウィンドウセッションは、その後のセキュアではないウィンドウ期間中に開始され、その期間中は、コード８９の実行により暗号化データ９６がサーバ８１に送信され、当該サーバ上で、エンティティアカウント９４の認証に続いて、対応する鍵９５を用いて、データＤ１～Ｄ７が復号され、それがセキュアなまたはセキュアではないチャネルを介して、サーバ８１からクライアント装置８２に送信される。好ましい形態において、データＤ１～Ｄ７は、クライアント装置８２上でフォーム構造９２に再投入される。その後、このデータは、クライアント装置８２で様々な機能に使用することができる。データＤ１～Ｄ７を、その後のセキュアではないウィンドウ期間の後のセッション中に修正をしてもよい。クライアント装置８２のユーザ又はクライアント装置自体がその後のセキュアではないウィンドウ期間を終了させると、図４Ａを参照して説明したように、データＤ１～Ｄ７がサーバ８１に送信され、図４Ｂを参照して説明したように、その後のセキュアなウィンドウ期間が開始される。

【００８０】

好ましい形態において、クライアント装置８２のユーザには、上述した手順を呼び出すか否かについての選択肢を与えることができる。

【００８１】

［クライアントサーバ環境］

図５を参照すると、典型的なクライアント／サーバ環境７０のトポロジがブロック図の形で示されており、この場合、少なくとも１つのクライアント装置７１と少なくとも１つのサーバ７２とを具えている。

【００８２】

クライアント装置７１は、データ通信チャネル７３を介してサーバ７２とデータ通信を行う。場合によって、このチャネル７３は一方向性であってよい。他の場合、チャネル７

３は双方向性であってよい。
【００８３】
好ましい形態において、チャネル７３又は少なくともその一部がインターネットを介して実行され、それにより、データがパケット形式で伝達され、それぞれのパケットは、少なくともターゲットアドレス情報を含むヘッダと、データ「ペイロード」を含むデータ部分とを具える。
【００８４】
好ましい形態において、クライアント７１のウェブページのデータは、サーバ７２に存在し、クライアントによるサーバへの要求に応じて、サーバ７２からクライアント７１に配信される。一部の形態において、データは一連のコマンドを具え、それらのコマンドは、クライアント７１上で実行されると、通常はビジュアルインタフェースにより、多くの場合はウェブページ７４の表示により、クライアント装置７１上でデータの通信をもたらす。
【００８５】
ウェブページ７４自体は、典型的には多数のデータ部分からなり、その一部分は、ウェブサーバ７２から受信したコマンドをクライアント７１が実行することにより構築され、一方で他の部分は、クライアント装置７１のユーザにより操作されるローカル入出力を介してクライアントに入力されるデータからなる。
【００８６】
現在使用されている共通のコマンド言語は、ＨＴＭＬ言語である。
【００８７】
［使用時における実施例１］
図６Ａ～６Ｐは、システムの例示的なアプリケーションをブロック図の形で示す。
【００８８】
［図６Ａ　初期に発生すること］
【００８９】
図６Ａを参照すると、アプリケーション１０１がユーザ装置１００、この場合スマートフォンで実行される。
【００９０】
［図６Ｂ　フォームの入力、サーバへの転送］
【００９１】
図６Ｂを参照すると、この例では、ユーザ１０２は、フライトの詳細及び支払の詳細を、ユーザ装置１００のタッチ可能なディスプレイ１０４に表示されるフォーム１０３のフィールド１０５に入力する。
【００９２】
この場合、７つのフィールドＦ１、Ｆ２．．．Ｆ７があり、各々がそれぞれのデータエントリＤ１、Ｄ２．．．Ｄ７を含む。
【００９３】
この場合、ユーザ装置１００は、Ｗｅｂサーバ１０６と第１のデータ通信を行い、ユーザ装置１００で開始した所定の取引１０８に関するデータが、ユーザ装置１００とサーバ１０６との間で交換される。
【００９４】
一部の形態において、サーバ１０６自体は、別の第２のデータ通信をサーバ１０７と行ってもよい。サーバ１０７は、例えば、取引１０８に係る当事者間での支払い承認を含む資金の移動を容易にする目的で、例えば金融仲介機関により利用される場合がある。
【００９５】
［図６Ｃ　データを保存せず、クリアリングハウスフォーム（サーバ１０７）にコピー／ＰＣＩ対応］
【００９６】
図６Ｃを参照すると、この例では、ユーザ１０２は、取引１０８をトリガするのに必要

なデータを構成するフィールドＦ１～Ｆ７にデータＤ１～データＤ７を入力し、それによりデータがサーバ１０６に電子的に伝達される。必要に応じて、サーバ１０６は、取引１０８の支払い承認の目的でサーバ１０７と通信を行う。

【００９７】

［図６Ｄ及び図６Ｅ　ユーザが、初めてアプリケーション１０１（「ウォレット」）でサイトを利用する場合であり、それ以外は同じである。］

【００９８】

図６Ｄ及び図６Ｅを参照すると、このプロセス中に、「将来取引を行うためにクレジットカードをセキュアに保存したいですか？」という案内をユーザに発行する。同様の案内を、ユーザが、例えば、金融データ、医療データ等を含む他の形式の支払いデータをセキュアに取扱うことを希望する他のデータに関して行ってもよい。

【００９９】

［図６Ｆから図６Ｐ‐鍵の生成及び使用手順］

【０１００】

図６Ｆを参照すると、暗号鍵が生成され、データが暗号化される。

【０１０１】

図６Ｇを参照すると、暗号鍵はユーザアカウントとともに保存される。

【０１０２】

図６Ｈを参照すると、暗号化されたカードデータがユーザの装置に保存され、キーチェーンにより保護される。

【０１０３】

図６Ｉを参照すると、鍵のみがサーバにあり、セキュアなデータがスマートフォンにあるように、サーバメモリがダンプされる。

【０１０４】

図６Ｊを参照すると、その後の接続で、ユーザが認証される。

【０１０５】

図６Ｋを参照すると、暗号化データがサーバに引き渡される。

【０１０６】

図６Ｌを参照すると、鍵がユーザのアカウントから取り出され、データが復号されてクリアリングハウスに伝達される。

【０１０７】

図６Ｍを参照すると、カードデータは新たな鍵で再暗号化される。

【０１０８】

図６Ｎを参照すると、新たな鍵がユーザのアカウントと共に保存される。

【０１０９】

図６Ｏを参照すると、新たな暗号化データのチャンクが、次回の取引のためにユーザの装置に保存される。

【０１１０】

図６Ｐを参照すると、サーバの鍵及びユーザの装置の暗号化データのみを残して、メモリをクリアする。

【０１１１】

［代替的実施形態］

例示的な実施形態では、データを使用する度に、データを新たな鍵で再暗号化する。代替的な実施形態では、データがフォームにおいて処理及び／又は使用されているか関わらず、クライアント及びサーバが接続すると、毎回又は複数回、データが再暗号化されることが確認できる。反対に、別の実施形態では、暗号化データが無限に同一の暗号鍵を用いていることが確認できる。

【０１１２】

例示の実施形態では、ＨＴＭＬ５ローカルストレージを用いて、暗号化データをクライアントに保存する。代替的な実施形態では、クライアントで利用可能であって、Ｗｅｂ対

応アプリケーション又はブラウザでサーバにアクセス可能である任意のストレージ手段を用いることができる。

【０１１３】

例示的な実施形態は、単一のドメインに保存及びリンクされたデータで用いられる。代替的な実施形態では、当業者に周知の手法を用いて、暗号化データが複数のドメインを通じてアクセスすることが可能となる。この例では、暗号化データが保存されるセキュアなドメイン領域のローカルストレージへのアクセスが可能なｉＦｒａｍｅを、クライアントにおいて異なるセキュアなドメイン空間にアクセス及び参照するウェブページ内に埋め込むことができるが、ｉＦｒａｍｅのセキュアな領域からのデータを、もとの又は他の関連のあるページに移動し、又は、もとの又は他の関連のあるページにより用いることができる。

【０１１４】

例示的な実施形態では、ユーザが、将来の使用のために任意でデータを暗号化及び保存できることを示す。代替的な実施形態では、この機能は、ローカルに暗号化してローカルに保存すべきデータをユーザが選択しなくてよい自動化プロセスであることが確認できる。

【図１】

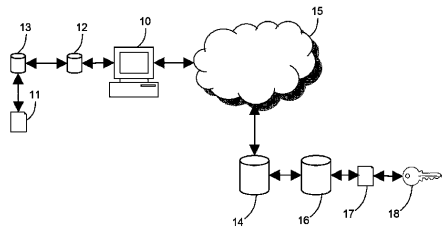


Figure 1

【図２】

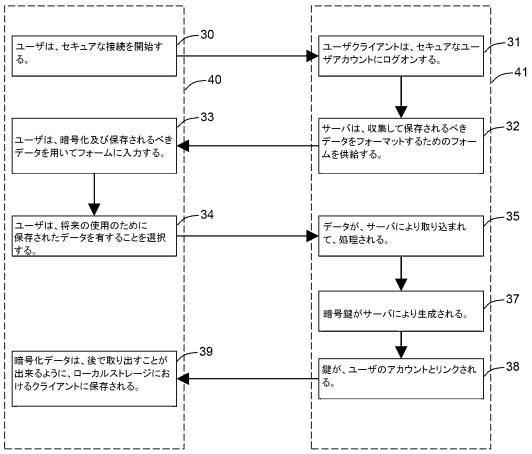


Figure 2

【図３】

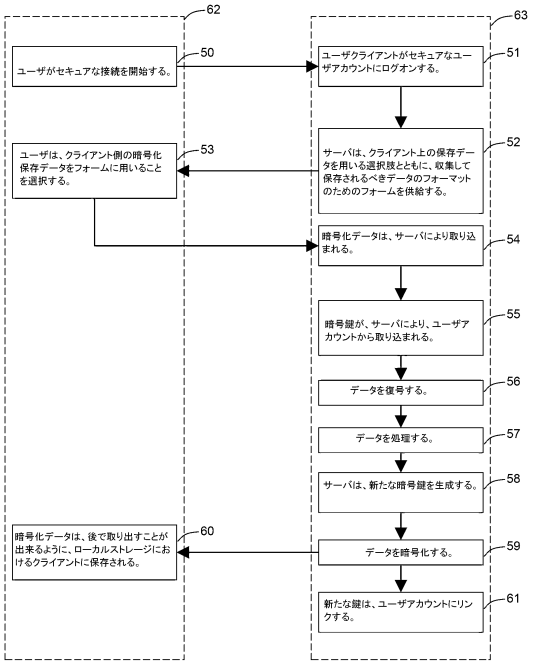
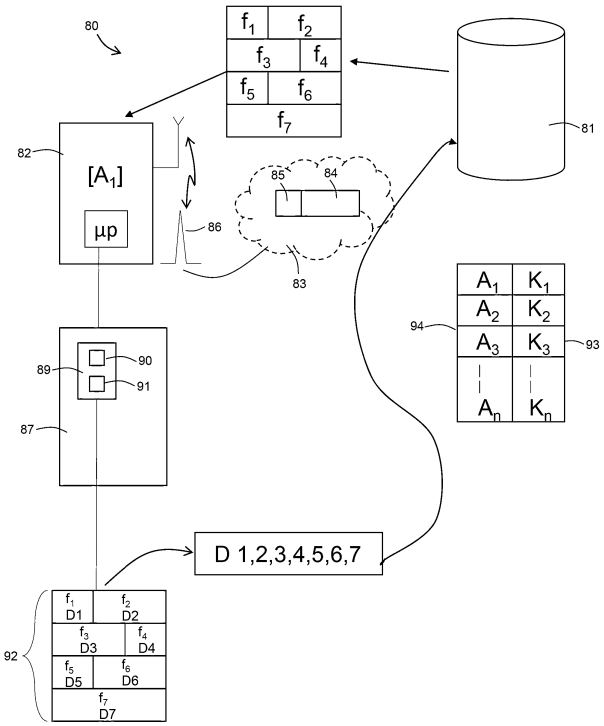


Figure 3

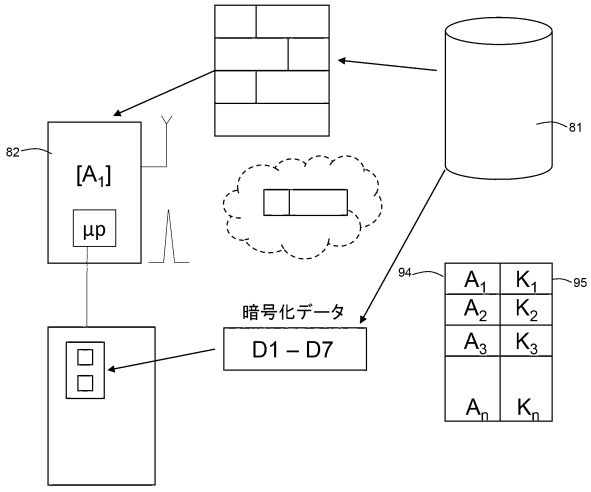
【図４Ａ】



セキュアではないウィンドウ期間

Fig. 4A

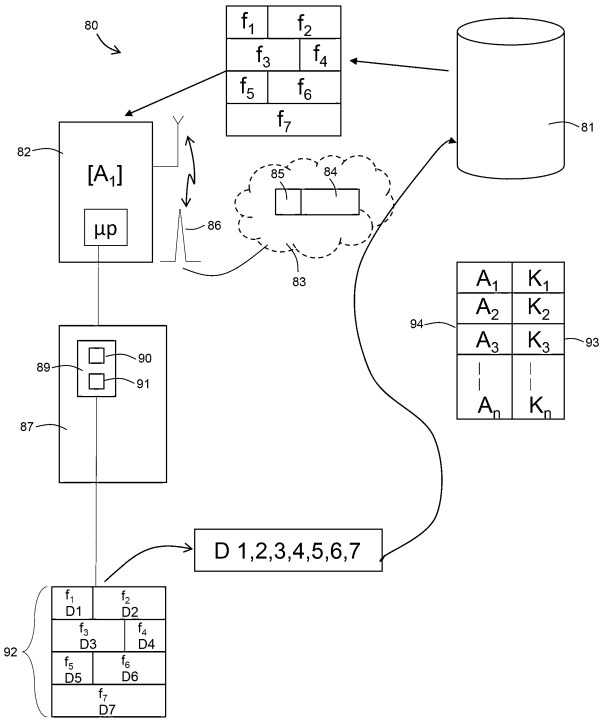
【図４Ｂ】



セキュアなウィンドウ期間

Fig. 4B

【図４Ｃ】



その後のセキュアではないウィンドウ期間

Fig. 4C

【図５】

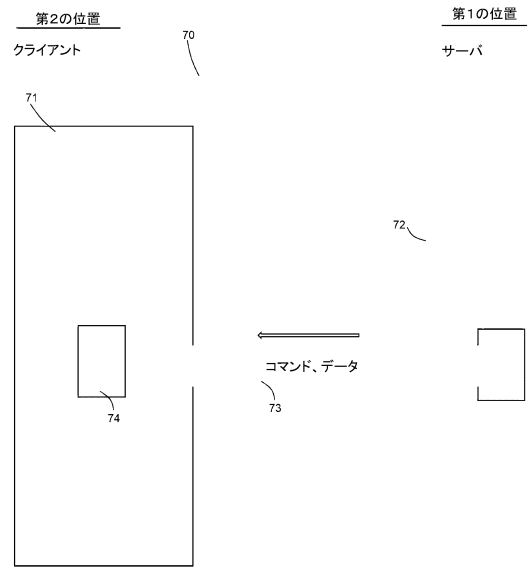


Fig. 5

【図６Ａ】

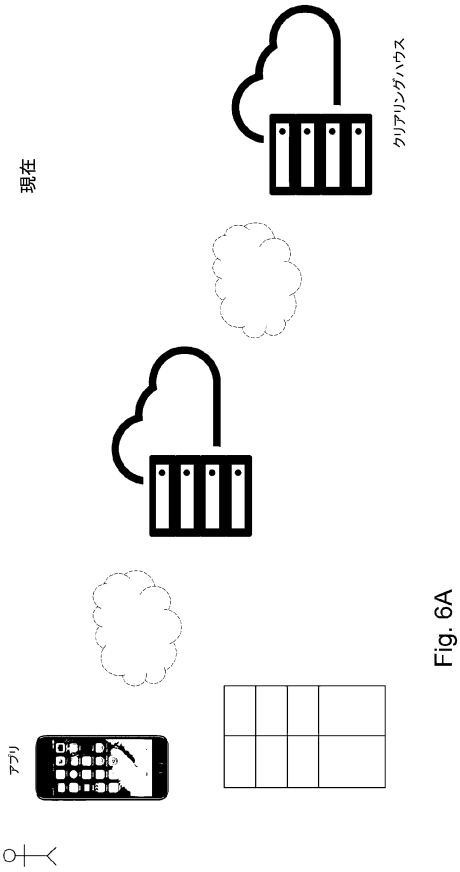


Fig. 6A

【図６Ｂ】

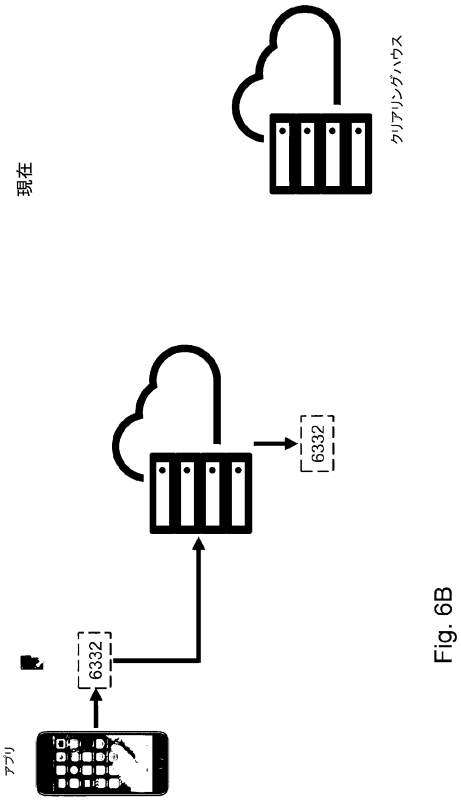


Fig. 6B

【図６Ｃ】

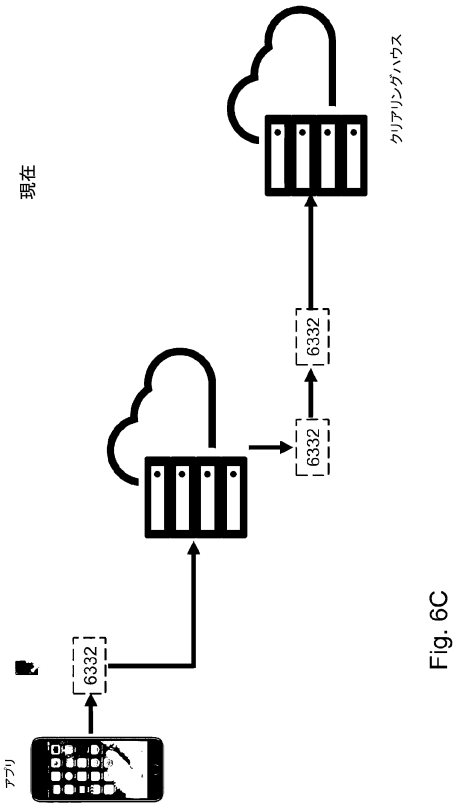


Fig. 6C

【図６Ｄ】

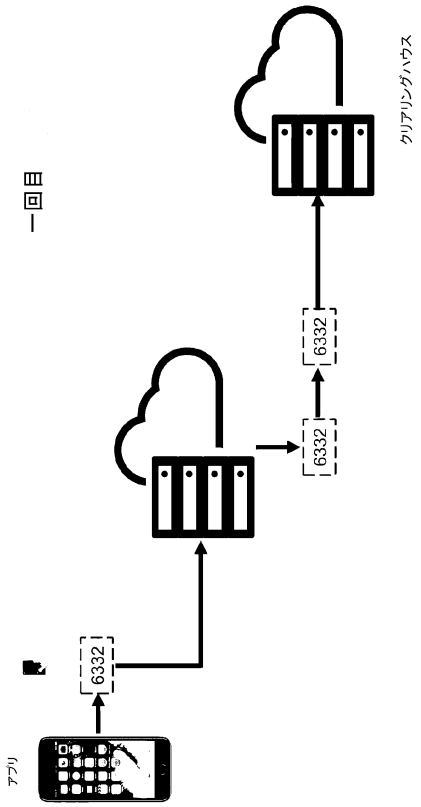


Fig. 6D

【図６Ｅ】

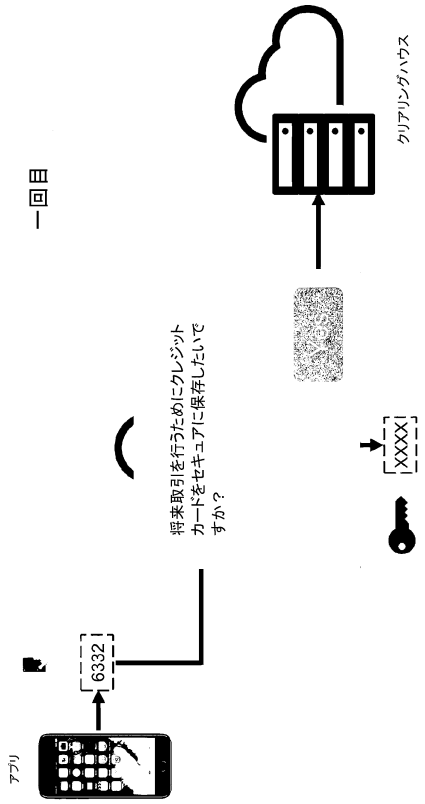


Fig. 6E

【図６Ｆ】

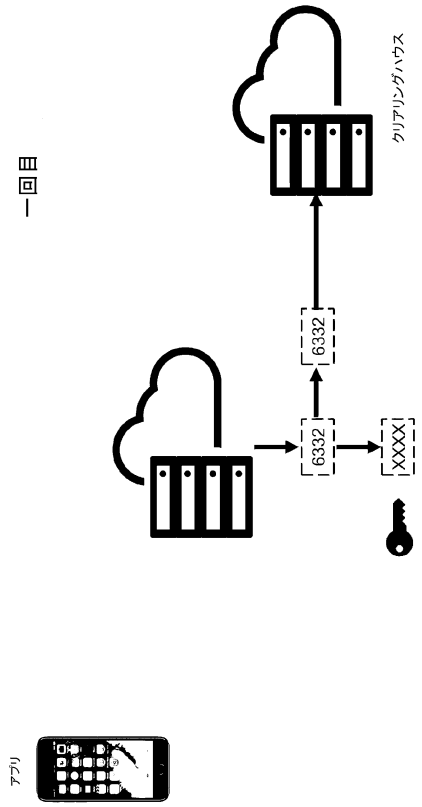


Fig. 6F

【図６Ｇ】

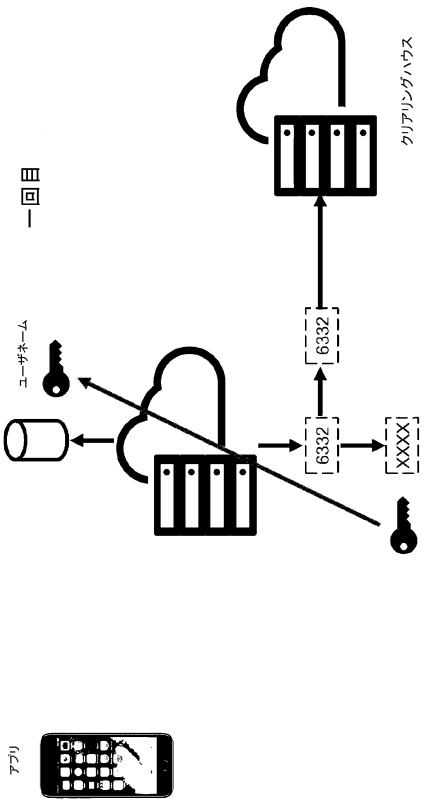


Fig. 6G

【図６Ｈ】

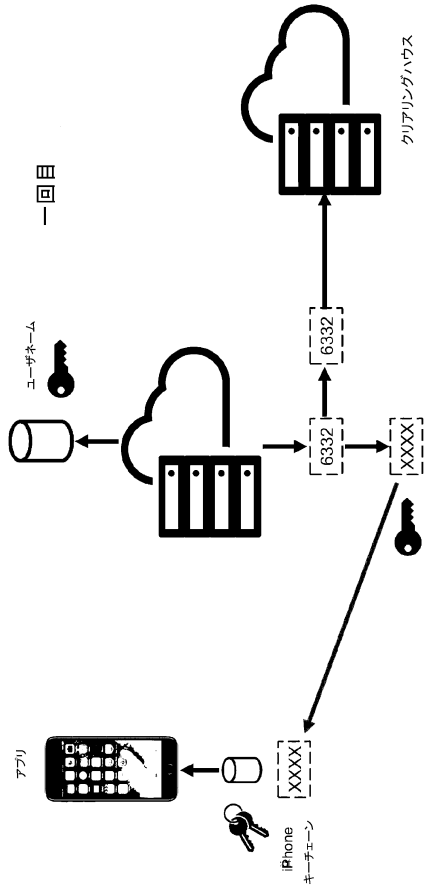


Fig. 6H

【図６Ｉ】

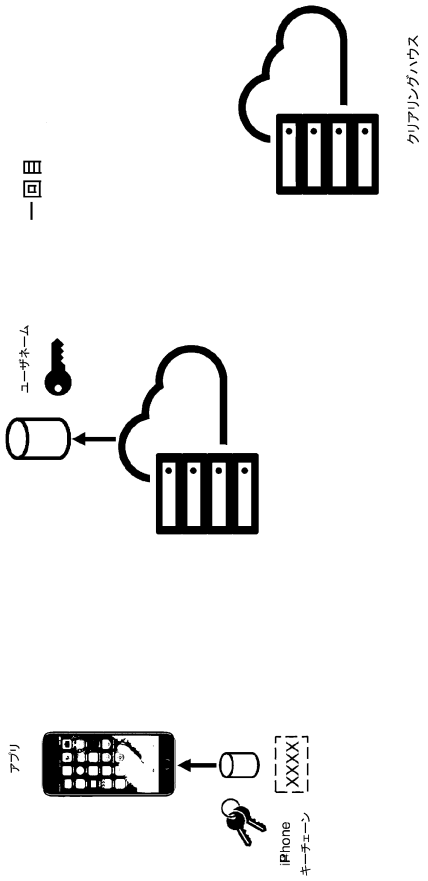


Fig. 6I

【図６Ｊ】

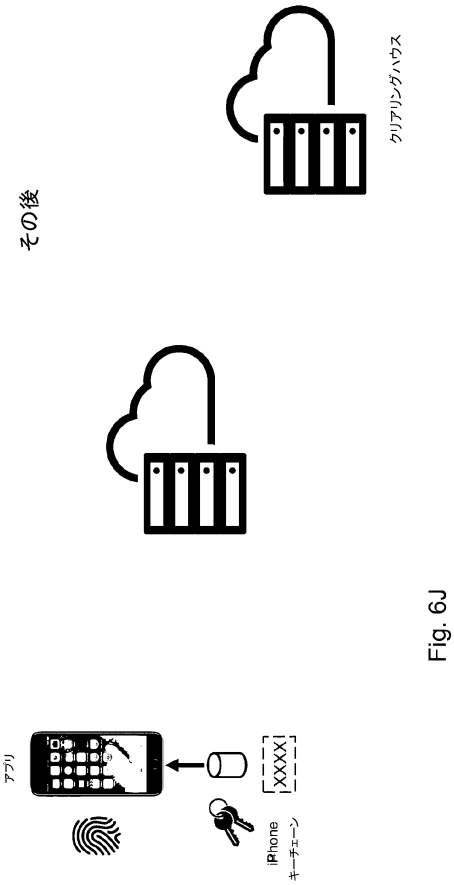


Fig. 6J

【図６Ｋ】

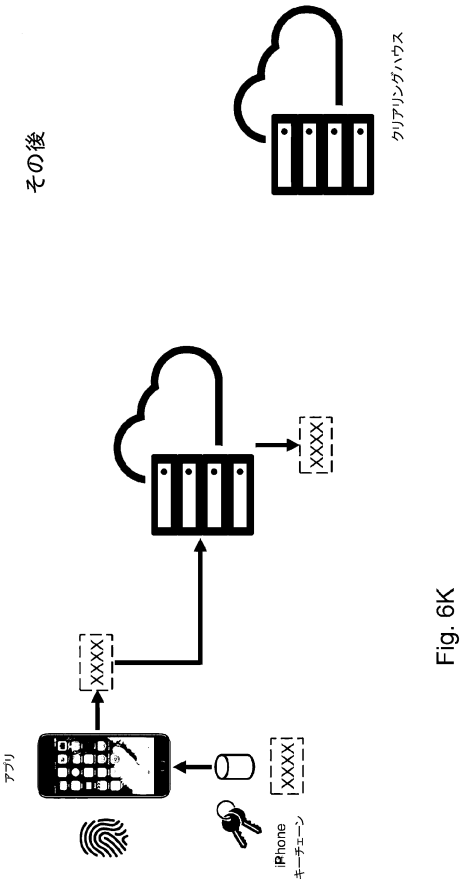


Fig. 6K

【図６Ｌ】

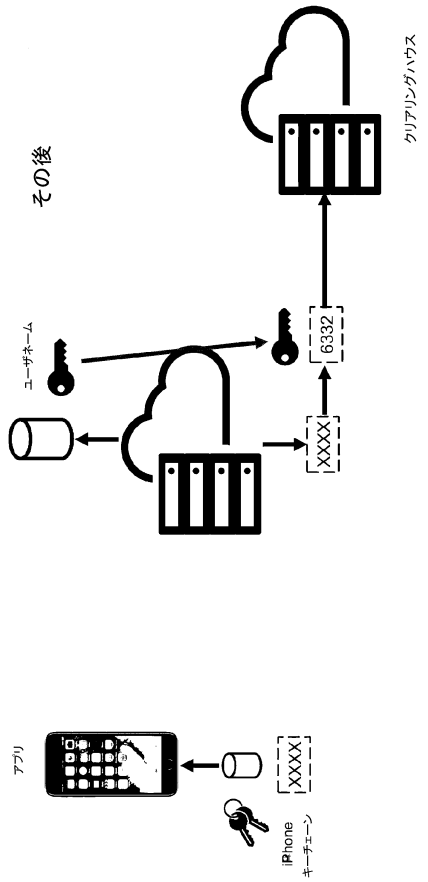


Fig. 6L

【図６Ｍ】

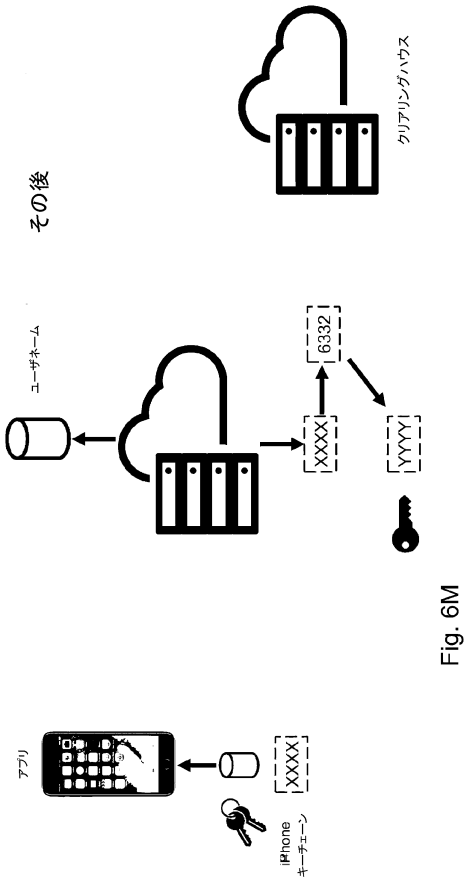


Fig. 6M

【図６Ｎ】

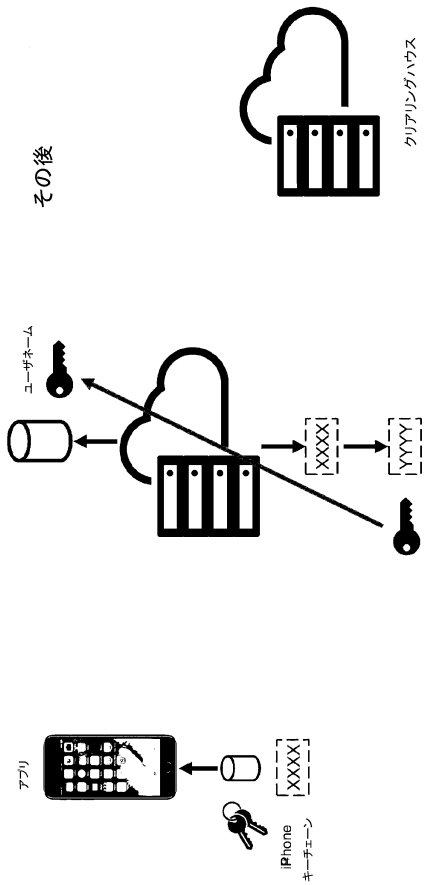


Fig. 6N

【図６Ｏ】

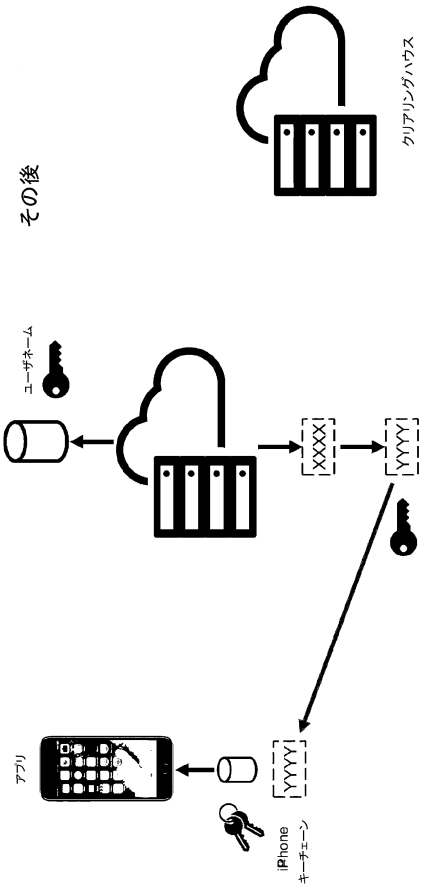


Fig. 6O

【図６Ｐ】

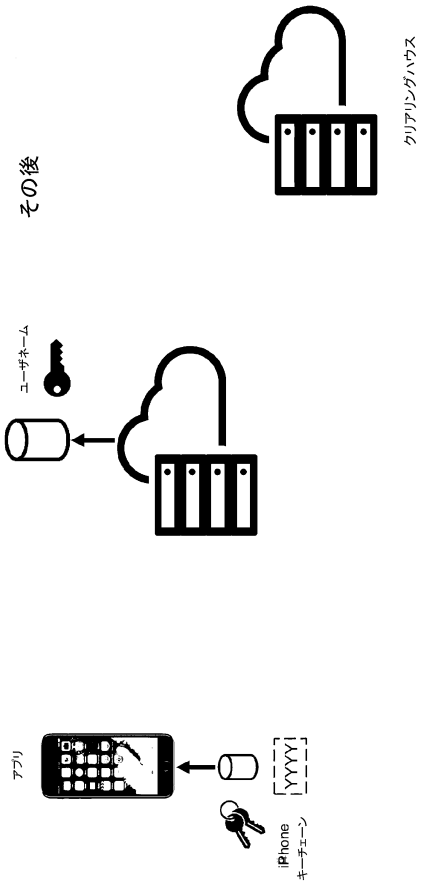


Fig. 6P

フロントページの続き

(56)参考文献 特表２０１３－５２９８０４（ＪＰ，Ａ）
特開２０１１－２７９１７（ＪＰ，Ａ）
特開２００９－１６４９９６（ＪＰ，Ａ）
特開２００６－９９３４８（ＪＰ，Ａ）
特開２０１０－１５７１４４（ＪＰ，Ａ）
特表２０１６－５０８６４３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１０
Ｇ０６Ｆ　２１／６０