【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】令和2年2月6日(2020.2.6)

【公表番号】特表2019-501592(P2019-501592A)
【公表日】平成31年1月17日(2019.1.17)
【年通号数】公開・登録公報2019-002
【出願番号】特願2018-533811(P2018-533811)
【国際特許分類】
Ｈ０４Ｌ　9/10　(2006.01)
Ｇ０６Ｆ　21/60　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６２１Ａ
Ｇ０６Ｆ　21/60　３２０

【手続補正書】
【提出日】令和1年12月18日(2019.12.18)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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。