

【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6部門第3区分
 【発行日】令和4年6月10日(2022.6.10)

【公開番号】特開2022-23942(P2022-23942A)
 【公開日】令和4年2月8日(2022.2.8)
 【年通号数】公開公報(特許)2022-023
 【出願番号】特願2021-176856(P2021-176856)
 【国際特許分類】

G 0 6 F 2 1 / 6 0 (2 0 1 3 . 0 1)
 H 0 4 L 9 / 3 6 (2 0 0 6 . 0 1)
 H 0 4 L 9 / 1 4 (2 0 0 6 . 0 1)
 H 0 4 L 1 2 / 6 6 (2 0 0 6 . 0 1)
 G 0 6 F 2 1 / 4 4 (2 0 1 3 . 0 1)

10

【 F I 】

G 0 6 F 2 1 / 6 0 3 2 0
 H 0 4 L 9 / 3 6
 H 0 4 L 9 / 1 4
 H 0 4 L 1 2 / 6 6
 G 0 6 F 2 1 / 4 4

20

【手続補正書】

【提出日】令和4年6月2日(2022.6.2)

【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】

30

少なくとも1つのメモリと、

第1計算装置と、

キーマネージャとを具えたシステムであって、

前記少なくとも1つのメモリは、複数のクライアントのうちの第1クライアントに関連する少なくとも1つのキーを記憶し、

前記第1計算装置は、暗号化ゲートウェイとして構成されて、クライアント側伝送プロトコルを用いて前記第1クライアントと通信し、リモート側伝送プロトコルを用いてリモートクラウド記憶装置またはリモートサーバーと通信し、前記第1計算装置は、少なくとも1つのプロセッサを具え、前記第1計算装置は、

少なくとも1つの認証因子を用いて前記第1クライアントを認証し、

40

ペイロード内のデータを前記第1クライアントから受信し、

前記クライアント側伝送プロトコルを用いて前記受信したデータを暗号復号化して、第1の暗号復号化したデータを提供し、

前記少なくとも1つのキーを用いて、前記第1の暗号復号化したデータを暗号化して、第1の暗号化したデータを提供し、

前記リモート側伝送プロトコルを用いて前記第1の暗号化したデータを暗号化して、第2の暗号化したデータを提供し、

前記第2の暗号化したデータを前記リモートクラウド記憶装置またはリモートサーバーに送信するか書き込む

ようにさらに構成され、

50

前記キーマネージャは、前記少なくとも1つのキーを、前記少なくとも1つのメモリに記憶するために、前記暗号化ゲートウェイに提供するように構成される、システム。

【請求項2】

前記暗号化ゲートウェイが、認証付き対称暗号化を用いて、前記第1の暗号復号化したデータを前記少なくとも1つのキーを用いて暗号化する、請求項1に記載のシステム。

【請求項3】

前記暗号化ゲートウェイが、前記リモート側伝送プロトコルを用いて前記データを暗号化する前に、前記クライアント・セッションのクライアント・セッションキーを用いて、前記第1クライアントからの前記ペイロードを暗号復号化する、請求項1に記載のシステム。

10

【請求項4】

前記リモートクラウド記憶装置または前記リモートサーバーへの前記暗号化接続に関連するクラウド・セッションキーを用いて、前記第1の暗号化したデータを前記暗号化ゲートウェイによって暗号化する、請求項1に記載のシステム。

【請求項5】

前記暗号化ゲートウェイが、前記ペイロードを前記第1クライアントから受信する前に、前記リモートクラウド記憶装置または前記リモートサーバーとの伝送セッションを設定し、前記暗号化ゲートウェイが、前記伝送セッションを用いて、複数のクライアント・アプリケーションからのデータを、前記リモートクラウド記憶装置または前記リモートサーバーに送信するか書き込む、請求項1に記載のシステム。

20

【請求項6】

前記暗号化ゲートウェイが、伝送接続内のヘッダを修正するか伝送接続内にヘッダを挿入して、前記第1クライアントをリモート接続に関連付ける、請求項5に記載のシステム。

【請求項7】

複数のクライアントのうちの第1クライアントに関連するキーを暗号化ゲートウェイのメモリに記憶するステップであって、前記第1クライアントはクライアント側伝送プロトコルを用いて前記暗号化ゲートウェイと通信するステップと、

暗号化ゲートウェイによって、第1の要求を、前記第1クライアントから受信するステップであって、前記第1の要求は、リモートクラウド記憶装置またはリモートサーバーからデータまたはファイル・オブジェクトを読み出すことの要求であり、前記リモートクラウド記憶装置または前記リモートサーバーはリモート側伝送プロトコルを用いて前記暗号化ゲートウェイと通信するステップと、

30

前記暗号化ゲートウェイによって、前記第1の要求に応答して、前記データまたは前記ファイル・オブジェクトを要求する第2の要求を前記リモートクラウド記憶装置または前記リモートサーバーに送信するステップと、

前記暗号化ゲートウェイによって、前記第2の要求に応答して、第1ペイロード内の前記データまたは前記ファイル・オブジェクトを前記リモートクラウド記憶装置または前記リモートサーバーから受信するステップであって、前記データまたは前記ファイル・オブジェクトは、前記リモート側伝送プロトコルを用いて暗号化されているステップと、

前記暗号化ゲートウェイの少なくとも1つのプロセッサによって、前記受信した前記第1ペイロード内の前記データまたは前記ファイル・オブジェクトを、前記リモート側伝送プロトコルを用いて暗号復号化して、第1の暗号復号化したデータを提供するステップと、前記暗号化ゲートウェイによって、前記第1クライアントに関連する前記キーを用いて前記第1の暗号復号化したデータを暗号復号化して、第2の暗号復号化したデータを提供するステップであって、前記キーは前記暗号化ゲートウェイの前記メモリから読み出されるステップと、

40

前記暗号化ゲートウェイによって、前記クライアント側伝送プロトコルを用いて前記第2の暗号復号化したデータを暗号化して、第1の暗号化したデータを提供するステップと、前記第1の暗号化したデータを、前記暗号化ゲートウェイから前記第1クライアントへ送信するステップと

50

を含む方法。

【請求項 8】

少なくとも 1 つのプロセッサと、
命令を記憶するメモリとを具えたシステムであって、
前記命令は、前記少なくとも 1 つのプロセッサに、
クライアント側伝送プロトコルを用いて、ペイロード内のデータを第 1 クライアントから受信し、
前記クライアント側伝送プロトコルを用いて、前記受信したデータを暗号復号化して、第 1 の暗号復号化したデータを提供し、
キーマネージャから少なくとも 1 つのキーを受信し、該少なくとも 1 つのキーは前記第 1 クライアントに関連し、
前記少なくとも 1 つのキーを用いて、前記第 1 の暗号復号化したデータを暗号化して、第 1 の暗号化したデータを提供し、
リモートクラウド記憶装置またはリモートサーバーに関連するリモート側伝送プロトコルを用いて、前記第 1 の暗号化したデータを暗号化して、第 2 の暗号化したデータを提供し
、
前記第 2 の暗号化したデータを、前記リモートクラウド記憶装置または前記リモートサーバーに送信するか書き込む
ことを指示するように構成されている、システム。

10

【請求項 9】

暗号化ゲートウェイのマルチプレクサまたはパケットエンジンによって、前記ペイロード内の前記データを前記第 1 クライアントから受信する、請求項 8 に記載のシステム。

20

【請求項 10】

暗号化ゲートウェイのパケットエンジンによって、前記第 2 の暗号化したデータを前記リモートクラウド記憶装置または前記リモートサーバーに送信するか書き込む、請求項 8 に記載のシステム。

30

40

50