(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-121256
(P2019-121256A)
(43)公開日　令和1年7月22日(2019.7.22)

(51)Int.Cl.			F I			テーマコード（参考）
G06N	3/08	(2006.01)	G06N	3/08		5J104
H04L	9/08	(2006.01)	H04L	9/00	601C	
			H04L	9/00	601E	

審査請求 未請求　請求項の数 6　OL　（全 16 頁）

(21)出願番号　特願2018-1656(P2018-1656)
(22)出願日　平成30年1月10日(2018.1.10)

特許法第３０条第２項適用申請有り　（刊行物名）　Ｎｅｔｗｏｒｋ　ａｎｄ　Ｓｙｓｔｅｍ　Ｓｅｃｕｒｉｔｙ　２０１７　予稿集　（公開者）　レ　チュウ　フォン　（発行日）　平成２９年７月２６日　（集会名）　国立研究開発法人情報通信研究機構　オープンハウス２０１７　（公開者）　レ　チュウ　フォン　（開催日）　平成２９年１１月９日　（集会名）　ＡＩＰ若手研究交流会　（公開者）　レ　チュウ　フォン　（開催日）　平成２９年１２月１９日

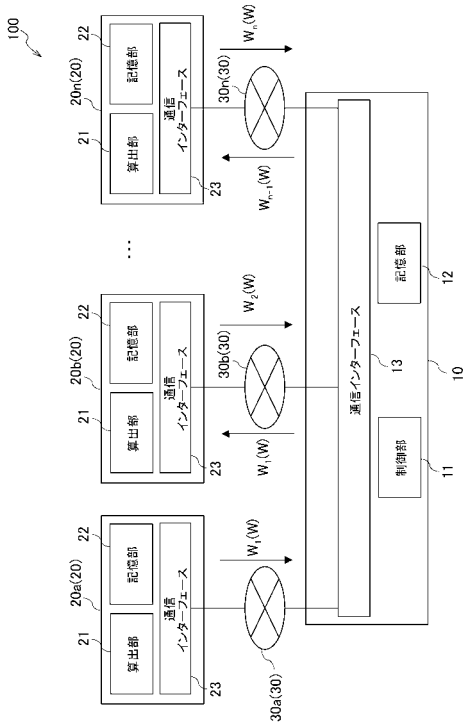
(71)出願人　301022471
国立研究開発法人情報通信研究機構
東京都小金井市貫井北町４－２－１
(74)代理人　100120868
弁理士　安彦　元
(72)発明者　レ　チュウ　フォン
東京都小金井市貫井北町４－２－１　国立研究開発法人情報通信研究機構内

Ｆターム(参考)　5J104 AA16　EA18　NA02　PA14

最終頁に続く

(54)【発明の名称】学習システム及び学習方法

(57)【要約】
【課題】学習効率の向上を図ることができる学習システム及び学習方法を提供する。
【解決手段】サーバ１０を介した複数のユーザ端末２０の間で、深層学習における再現性の最適化を行う学習システム１００であって、複数の前記ユーザ端末２０に含まれる第１ユーザ端末２０ａの有する第１参照データと、予め取得された重み変数Wとを参照し、第１重み変数W_1を算出する第１算出手段Ｓ１１０と、前記サーバ１０を介して前記第１重み変数W_1を、前記第１ユーザ端末２０ａから複数の前記ユーザ端末２０に含まれる第２ユーザ端末２０ｂに送信する送受信手段Ｓ１２０と、前記第２ユーザ端末２０ｂの有する第２参照データと、前記第１重み変数W_1とを参照し、第２重み変数W_2を算出する第２算出手段Ｓ１３０と、を備えることを特徴とする。
【選択図】図１



【特許請求の範囲】
【請求項１】
サーバを介した複数のユーザ端末の間で、深層学習における再現性の最適化を行う学習システムであって、
複数の前記ユーザ端末に含まれる第１ユーザ端末の有する第１参照データと、予め取得された重み変数とを参照し、第１重み変数を算出する第１算出手段と、
前記サーバを介して前記第１重み変数を、前記第１ユーザ端末から複数の前記ユーザ端末に含まれる第２ユーザ端末に送信する送受信手段と、
前記第２ユーザ端末の有する第２参照データと、前記第１重み変数とを参照し、第２重み変数を算出する第２算出手段と、
を備えることを特徴とする学習システム。
【請求項２】
前記送受信手段は、前記第１重み変数を、複数の前記ユーザ端末のうち、前記第２ユーザ端末のみに送信すること
を特徴とする請求項１記載の学習システム。
【請求項３】
複数の前記ユーザ端末に取得される共通鍵暗号を生成する生成手段をさらに備え、
前記第１算出手段は、前記第１ユーザ端末において、前記共通鍵暗号を用いて、前記第１重み変数を暗号化する暗号化手段を有し、
前記送受信手段は、
前記第２ユーザ端末において、前記共通鍵暗号を用いて、暗号化された前記第１重み変数を復号する復号手段を有し、
前記暗号化された前記第１重み変数を、前記第１ユーザ端末から前記サーバに送信し、
前記暗号化された前記第１重み変数を、前記サーバから前記第２ユーザ端末に送信すること
を特徴とする請求項１又は２記載の学習システム。
【請求項４】
前記第１重み変数及び前記第２重み変数は、確率的勾配降下法を用いて算出され、
前記第１算出手段は、
前記第１参照データと、前記重み変数とを参照して第１勾配情報を導出し、
前記第１勾配情報及び前記重み変数に基づく前記第１重み変数を算出し、
前記第２算出手段は、
前記第２参照データと、前記第１重み変数とを参照して第２勾配情報を導出し、
前記第２勾配情報及び前記第１重み変数に基づく前記第２重み変数を算出すること
を特徴とする請求項１～３の何れか１項記載の学習システム。
【請求項５】
前記送受信手段は、複数の前記ユーザ端末のうち、１つのユーザ端末を前記第２ユーザ端末として、前記サーバ内において設定すること
を特徴とする請求項１～４の何れか１項記載の学習システム。
【請求項６】
サーバを介した複数のユーザ端末の間で、深層学習における再現性の最適化を行う学習方法であって、
複数の前記ユーザ端末に含まれる第１ユーザ端末の有する第１参照データと、予め取得された重み変数とを参照し、第１重み変数を算出する第１算出ステップと、
前記サーバを介して前記第１重み変数を、前記第１ユーザ端末から複数の前記ユーザ端末に含まれる第２ユーザ端末に送信する送受信ステップと、
前記第２ユーザ端末の有する第２参照データと、前記第１重み変数とを参照し、第２重み変数を算出する第２算出ステップと、
を備えることを特徴とする学習方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サーバを介した複数のユーザ端末の間で、深層学習における再現性の最適化を行う学習システム及び学習方法に関するものである。
【背景技術】
【０００２】
近年、深層学習（deep learning）と呼ばれる機械学習の手法は、学術界及び産業界を含む幅広い分野で期待されている。深層学習に関する技術のうち、複数のユーザ端末が保有する参照データに基づき、深層学習を分散させて実行する方法が注目を集めており、分散協調学習や分散深層学習等と呼ばれている。この場合、例えば確率的勾配降下法（SGD: Stochastic gradient descent）等を用いることで、再現性の最適化が行われている。
【０００３】
上述した技術として、例えば非特許文献１では、各ユーザ端末に接続された中央サーバが、ニューラルネットワークの有するノード間の重み変数を更新する技術が開示されている。非特許文献１では、各ユーザは、各ユーザ端末の有する参照データを参照して勾配情報を導出し、導出した勾配を中央サーバに送信する。中央サーバは、各ユーザ端末において導出された勾配情報に基づいて重み変数を算出し、算出した重み変数を各ユーザ端末に送信する。
【０００４】
また、特許文献１では、量子化勾配の情報を用いる分散深層学習装置が提案されている。特許文献１では、複数の学習装置との間で量子化勾配を交換して分散して深層学習を行うための分散深層学習装置であって、他の学習装置との間で通信によって量子化勾配を交換する通信部と、現在のパラメータの勾配を計算する勾配計算部と、勾配計算部で求めた勾配に対して、前回勾配を量子化した時の剰余分に所定倍率を乗算したものを加算する量子化剰余加算部と、量子化剰余加算部によって所定倍後の剰余分が加算された勾配を量子化する勾配量子化部と、通信部で受信した量子化勾配を本来の精度の勾配に復元する勾配復元部と、勾配量子化部において勾配を量子化した時の剰余分を記憶する量子化剰余記憶部と、通信部で集められた勾配を集約して集約された勾配を計算する勾配集約部と、勾配集約部で集約された勾配に基づいてパラメータを更新するパラメータ更新部とを備える分散深層学習装置について開示されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特許第６２２７８１３号公報
【非特許文献】
【０００６】
【非特許文献１】Reza Shokri, Vitaly Shmatikov: Privacy-Preserving Deep Learning. ACM Conference on Computer and Communications Security 2015: 1310-1321
【発明の概要】
【発明が解決しようとする課題】
【０００７】
ここで、上述した開示技術では、各ユーザ端末等で導出された勾配情報を用いて、深層学習における再現性の最適化を行っている。しかしながら、勾配情報は、入力データ（参照データ）や重み変数等に基づく関数を含み、データ容量が大きい。このため、深層学習における再現性の向上等に伴い、送受信に必要となる勾配情報の容量が飛躍的に増大する可能性がある。これにより、端末間における勾配情報の送受信に時間を浪費し、学習効率の低下が懸念として挙げられる。
【０００８】
そこで本発明は、上述した問題点に鑑みて案出されたものであり、その目的とするとこ

ろは、学習効率の向上を図ることができる学習システム及び学習方法を提供することにある。

【課題を解決するための手段】

【０００９】

本発明者らは、上述した問題点を解決するために、サーバを介した複数のユーザ端末の間で、深層学習における再現性の最適化を行う学習システム及び学習方法を発明した。学習システムは、第１算出手段と、送受信手段と、第２算出手段とを備える。第１算出手段は、複数のユーザ端末に含まれる第１ユーザ端末の有する第１参照データと、予め取得された重み変数とを参照し、第１重み変数を算出する。送受信手段は、サーバを介して第１重み変数を、第１ユーザ端末から複数のユーザ端末に含まれる第２ユーザ端末に送信する。第２算出手段は、第２ユーザ端末の有する第２参照データと、第１重み変数とを参照し、第２重み変数を算出する。

【００１０】

請求項１に記載の学習システムは、サーバを介した複数のユーザ端末の間で、深層学習における再現性の最適化を行う学習システムであって、複数の前記ユーザ端末に含まれる第１ユーザ端末の有する第１参照データと、予め取得された重み変数とを参照し、第１重み変数を算出する第１算出手段と、前記サーバを介して前記第１重み変数を、前記第１ユーザ端末から複数の前記ユーザ端末に含まれる第２ユーザ端末に送信する送受信手段と、前記第２ユーザ端末の有する第２参照データと、前記第１重み変数とを参照し、第２重み変数を算出する第２算出手段と、を備えることを特徴とする。

【００１１】

請求項２に記載の学習システムは、請求項１記載の学習システムにおいて、前記送受信手段は、前記第１重み変数を、複数の前記ユーザ端末のうち、前記第２ユーザ端末のみに送信することを特徴とする。

【００１２】

請求項３に記載の学習システムは、請求項１又は請求項２記載の学習システムにおいて、複数の前記ユーザ端末に取得される共通鍵暗号を生成する生成手段をさらに備え、前記第１算出手段は、前記第１ユーザ端末において、前記共通鍵暗号を用いて、前記第１重み変数を暗号化する暗号化手段を有し、前記送受信手段は、前記第２ユーザ端末において、前記共通鍵暗号を用いて、暗号化された前記第１重み変数を復号する復号手段を有し、前記暗号化された前記第１重み変数を、前記第１ユーザ端末から前記サーバに送信し、前記暗号化された前記第１重み変数を、前記サーバから前記第２ユーザ端末に送信することを特徴とする。

【００１３】

請求項４に記載の学習システムは、請求項１～請求項３の何れか記載の学習システムにおいて、前記第１重み変数及び前記第２重み変数は、確率的勾配降下法を用いて算出され、前記第１算出手段は、前記第１参照データと、前記重み変数とを参照して第１勾配情報を導出し、前記第１勾配情報及び前記重み変数に基づく前記第１重み変数を算出し、前記第２算出手段は、前記第２参照データと、前記第１重み変数とを参照して第２勾配情報を導出し、前記第２勾配情報及び前記第１重み変数に基づく前記第２重み変数を算出することを特徴とする。

【００１４】

請求項５に記載の学習システムは、請求項１～請求項４の何れか記載の学習システムにおいて、前記送受信手段は、複数の前記ユーザ端末のうち、１つのユーザ端末を前記第２ユーザ端末として、前記サーバ内において設定することを特徴とする。

【００１５】

請求項６に記載の学習方法は、サーバを介した複数のユーザ端末の間で、深層学習における再現性の最適化を行う学習方法であって、複数の前記ユーザ端末に含まれる第１ユーザ端末の有する第１参照データと、予め取得された重み変数とを参照し、第１重み変数を算出する第１算出ステップと、前記サーバを介して前記第１重み変数を、前記第１ユーザ

端末から複数の前記ユーザ端末に含まれる第２ユーザ端末に送信する送受信ステップと、前記第２ユーザ端末の有する第２参照データと、前記第１重み変数とを参照し、第２重み変数を算出する第２算出ステップと、を備えることを特徴とする。

【発明の効果】

【００１６】

上述した構成からなる本発明によれば、送受信手段は、第１重み変数を、第１ユーザ端末から第２ユーザ端末に送信する。すなわち、各ユーザ端末で算出された重み変数を、サーバを介したユーザ端末間で送受信し、深層学習における再現性の最適化を行う。このため、勾配情報をユーザ端末間で送受信した場合に比べて、送受信に必要となるデータ容量を大幅に縮小させることができる。これにより、ユーザ端末間におけるデータの送受信に費やす時間を削減でき、学習効率の向上を図ることが可能となる。

【００１７】

また、上述した構成からなる本発明によれば、送受信手段は、サーバを介して第１重み変数を、第１ユーザ端末から第２ユーザ端末に送信する。すなわち、各ユーザ端末間において直接重み変数の送受信を行わない。このため、例えば第２ユーザ端末に送信される第１重み変数が、第１ユーザ端末において算出されたことを、他のユーザに対して秘匿することができる。これにより、ユーザ端末を保有するユーザに起因する情報の漏洩を抑制することが可能となる。

【００１８】

また、上述した構成からなる本発明によれば、送受信手段は、第１重み変数を、第２ユーザ端末のみに送信する。すなわち、各ユーザ端末において順番に重み変数が算出される手段を備える。このため、１つのユーザ端末において算出された勾配情報等を、複数のユーザ端末等に送信する手段に比べて、再現性の精度を飛躍的に向上させることができる。これにより、学習効率の向上を容易に図ることが可能となる。また、勾配情報等を複数のユーザ端末等に送信する必要が無いため、データの送受信に費やす時間をさらに削減することが可能となる。

【００１９】

また、上述した構成からなる本発明によれば、送受信手段は、暗号化された第１重み変数を、サーバを介して第１ユーザ端末から第２ユーザ端末に送信する。このため、サーバでは暗号化された第１重み変数を復元できず、第１重み変数の内容を把握することができない。これにより、サーバを保有する管理者等に起因する情報の漏洩を抑制することが可能となる。

【００２０】

また、上述した構成からなる本発明によれば、第１算出手段は、第１勾配情報及び重み変数に基づく第１重み変数を算出する。すなわち、ユーザ端末毎に勾配情報を導出し、重み変数を算出する。このため、勾配情報に含まれるユーザ端末毎に有する参照データを推定できる情報は、他のユーザ端末等に送信する必要が無い。これにより、各ユーザ端末の有ずる参照データの漏洩を抑制することが可能となる。

【００２１】

また、上述した構成からなる本発明によれば、送受信手段は、複数のユーザ端末のうち、１つのユーザ端末を第２ユーザ端末として、サーバ内において設定する。このため、重み変数が送受信される順番を、ユーザに知られないようにすることができる。これにより、ユーザ端末を保有するユーザに起因する情報の漏洩を容易に抑制することが可能となる。

【図面の簡単な説明】

【００２２】

【図１】本発明が適用される学習システムの一例を示す模式図である。

【図２】本実施形態における学習の対象となるニューラルネットワークの一例を示す模式図である。

【図３】本発明が適用される学習システムの動作の一例を示すフローチャートである。

【図４】ユーザ端末等の構成の一例を示す模式図である。
【図５】本発明が適用される学習システムの変形例を示す模式図である。
【図６】本発明が適用される学習システムの動作の変形例を示すフローチャートである。
【発明を実施するための形態】
【００２３】
（実施形態：学習システム１００の構成）
以下、本発明の実施形態としての学習システムについて説明する。図１は、本実施形態における学習システム１００の一例を示す模式図である。
【００２４】
図１に示すように、学習システム１００は、サーバ１０と、複数のユーザ端末２０とを備え、各ユーザ端末２０は、例えば公衆通信網３０を介してサーバ１０に接続される。学習システム１００は、サーバ１０を介した複数のユーザ端末２０の間で、深層学習における再現性の最適化を行うために用いられる。
【００２５】
学習システム１００では、１つのユーザ端末２０において深層学習を行い、学習した結果を重み変数Ｗとして算出し、サーバ１０を介して他のユーザ端末２０に送信する。他のユーザ端末２０は、受信した重み変数Ｗを参照し、新たな重み変数Ｗを算出する。この動作を繰り返し行うことで、深層学習における再現性の最適化を行う。
【００２６】
各ユーザ端末２０が重み変数Ｗを算出するとき、予め取得した重み変数Ｗに加えて、各ユーザ端末２０の有する参照データを参照する。このため、各ユーザ端末２０の有する参照データを１つのユーザ端末２０等に集約することなく、精度の高い学習を実現することができる。各ユーザ端末２０は、例えばそれぞれ異なる参照データを有することで、深層学習に用いる参照データ数を増やすことができる。
【００２７】
＜ニューラルネットワーク＞
図２は、本実施形態における学習の対象となるニューラルネットワークの一例を示す模式図である。図２に示すように、ニューラルネットワークは、第１層に入力層（Input layer）と、第２層及び第３層に隠れ層（Hidden layers）と、第４層に出力層（Output layer）とを有し、各層は複数のノードＮを有する。なお、図２では、２層の隠れ層、並びに第１層に６つのノードＮ１１～Ｎ１６、第２層に４つのノードＮ２１～Ｎ２４、第３層に６つのノードＮ３１～Ｎ３６、及び第４層に４つのノードＮ４１～Ｎ４４を示しているが、隠れ層の総数及び各層におけるノードＮの数は任意である。各ユーザ端末２０は、それぞれ等しい層数及びノード数のニューラルネットワークを有する。
【００２８】
各ノードＮは、例えばアクティブ化関数と関連付けられる。アクティブ化関数として、例えば下記の［数１］に示すランプ関数のほか、例えばhyperbolic tangent、sigmoid等が用いられる。また、例えば任意のノードＮを、上述したアクティブ化関数を関連付けられないバイアス項としてもよい（図２ではＮ１６、Ｎ２４、Ｎ３６）。
【数１】

$$f(z)=\max\{0,z\}$$

【００２９】
＜重み変数Ｗ＞
各ノードＮは、隣接する層のノードＮに対して重み変数Ｗで紐づけられている（図２の矢印）。重み変数Ｗは、ノードＮの間毎に異なる値を示し、深層学習における再現性に影響する変数である。重み変数Ｗは、例えば行列で示される。重み変数Ｗを各ユーザ端末２０において順番に算出し、更新することで、深層学習における再現性の精度向上を図ることができる。
【００３０】

重み変数Ｗは、例えば確率的勾配降下法（SGD: Stochastic Gradient Descent）を用いて算出される。この場合、各ユーザ端末２０では、ユーザ端末２０毎に有する参照データと、予め取得された重み変数Ｗとを参照して、下記の［数２］に示す勾配情報Ｇを導出する。その後、勾配情報Ｇ及び重み変数Ｗに基づき、下記の［数３］に示す重み変数W_uを算出（更新）する。この演算をユーザ端末２０毎に繰り返すことにより、［数２］に示すコスト関数Ｊを最小化する重み変数Ｗが算出され、深層学習における再現性の最適化を実現できる。なお、［数３］で示した重み変数W_u及び重み変数Ｗの違いは、更新前後の違いを示すのみであるため、以下の説明では重み変数W_uを単にＷと記載する場合がある。

【数２】

$$G = \frac{\delta J(W, x, y)}{\delta W}$$

ここで、ｘは参照データの入力値を示し、ｙは参照データの真理値を示し、Ｊは入力値ｘ、真理値ｙ、及び予め取得された重み変数Ｗについて定義されたコスト関数を示す。

【数３】

$$W_u \leftarrow W - \alpha \cdot G$$

ここで、αは任意の学習率を示す。なお、本実施形態では、ユーザ端末２０毎に異なる学習率αが設定されてもよい。

【００３１】

本実施形態によれば、各ユーザ端末２０において順番に重み変数Ｗを算出する。このため、ユーザ端末２０間に送受信するデータ容量を最小限に抑制することができる。すなわち、重み変数Ｗは、ユーザ端末２０毎に有する参照データについて定義された関数等を含まないため、勾配情報Ｇに比べてデータ容量が小さい傾向を示す。このため、ユーザ端末２０間におけるデータの送受信に費やす時間を削減できる。

【００３２】

また、本実施形態によれば、重み変数Ｗの算出及び送信を、１つのユーザ端末２０毎に行う。すなわち、本実施形態における学習システム１００では、従来用いられている１つのユーザ端末において算出された勾配情報Ｇ等を、複数のユーザ端末等に送信して並列演算する手段（非同期型）ではなく、同期型の最適化が用いられる。このため、再現性の精度を飛躍的に向上させることができる。

【００３３】

＜サーバ１０＞

サーバ１０は、図１に示すように、複数のユーザ端末２０と接続され、重み変数Ｗ等の各種情報を送受信及び保存する。サーバ１０は、例えばクラウドサーバのように、管理者等に代わって各種情報の記憶等を行う第三者機関（業務委託先等）が保有するサーバでもよい。

【００３４】

サーバ１０は、例えばＳＳＬ／ＴＬＳ（Secure Sockets Layer / Transport Layer Security）等の暗号化技術を利用して、各ユーザ端末２０とそれぞれ独立して接続される。このため、ユーザ端末２０同士の接続を独立させた状態で、サーバ１０を介して各種情報を送受信できる。これにより、ユーザ端末２０間における各種情報の送受信は、必ずサーバ１０を介して行われるようにすることができる。

【００３５】

サーバ１０は、制御部１１と、記憶部１２と、通信インターフェース１３とを有する。制御部１１は、サーバ１０内の各種制御を行う。制御部１１は、例えば複数のユーザ端末２０に対して、重み変数Ｗを送信する順番を制御する。この場合、複数のユーザ端末２０の有するユーザは、サーバ１０から受信した重み変数Ｗがどこのユーザ端末２０で算出されたかを、確認することができない。

【００３６】
記憶部１２は、ユーザ端末２０から受信した重み変数Ｗ等の各種情報を記憶する。通信インターフェース１３は、公衆通信網３０を介してユーザ端末２０と接続され、重み変数Ｗ等の各種情報を送受信する。
【００３７】
＜ユーザ端末２０＞
ユーザ端末２０は、深層学習における再現性の最適化に必要となる重み変数Ｗを算出する。ユーザ端末２０は、深層学習に必要となる参照データを有し、ユーザ端末２０毎に異なる参照データを有する。このため、深層学習における再現性の最適化は、ユーザ端末２０の数によって得られる精度が変わる。なお、図１ではｎつのユーザ端末２０（２０ａ、２０ｂ、・・・、２０ｎ）を示しているが、ユーザ端末２０の数は任意である。
【００３８】
ユーザ端末２０は、算出部２１と、記憶部２２と、通信インターフェース２３とを有する。算出部２１は、ユーザ端末２０毎に有する参照データと、予め取得された重み変数Ｗとを参照し、重み変数Ｗを算出する。算出部２１は、例えば確率的勾配降下法を用いた場合、［数２］に示した勾配情報Ｇを導出し、［数３］に示した重み変数W_u（Ｗ）を算出する。
【００３９】
記憶部２２は、参照データや、重み変数Ｗ等の各種情報を記憶する。通信インターフェース２３は、公衆通信網３０を介してサーバ１０と接続され、重み変数Ｗ等の各種情報を送受信する。
【００４０】
＜公衆通信網３０＞
公衆通信網３０（ネットワーク）は、サーバ１０等が通信回路を介して接続されるインターネット網等である。公衆通信網３０は、いわゆる光ファイバ通信網で構成されてもよい。また、公衆通信網３０は、有線通信網には限定されず、無線通信網で実現してもよい。公衆通信網３０は、例えば図１に示すように、ユーザ端末２０毎に複数の通信網３０ａ、３０ｂ、・・・、３０ｎを有してもよく、各ユーザ端末２０とサーバ１０との各種情報の送受信が実現できれば、任意の構成を備えることができる。
【００４１】
（実施形態：学習システム１００の動作）
次に、本実施形態における学習システム１００の動作について説明する。図３は、本実施形態における学習システム１００の動作の一例を示すフローチャートである。
【００４２】
学習システム１００の動作は、第１算出手段Ｓ１１０と、送受信手段Ｓ１２０と、第２算出手段Ｓ１３０とを備える。第１算出手段Ｓ１１０は、例えば初期値設定手段Ｓ１１１を有する。送受信手段Ｓ１２０は、例えば第１手段Ｓ１２１と、第２手段Ｓ１２２とを有する。
【００４３】
＜第１算出手段：Ｓ１１０＞
先ず、複数のユーザ端末２０に含まれる１つのユーザ端末２０（以下、第１ユーザ端末２０ａとする）において、重み変数Ｗ（以下、第１重み変数W_1とする）を算出する。第１ユーザ端末２０ａの算出部２１は、第１参照データと、予め取得された重み変数Ｗとを参照し、第１重み変数W_1を算出する。ここで、予め取得された重み変数Ｗは、例えば初期値として算出部２１で設定されてもよい（初期値設定手段Ｓ１１１）ほか、例えば他のユーザ端末２０において算出された重み変数Ｗを取得してもよい。第１ユーザ端末２０ａの記憶部２２は、例えば算出した第１重み変数W_1を記憶する。
【００４４】
第１重み変数W_1を算出するとき、例えば上述した確率的勾配降下法を用いてもよい。この場合、第１ユーザ端末２０ａの算出部２１は、第１参照データと、重み変数Ｗとを参

照して、［数２］に示した勾配情報Ｇ（以下、第１勾配情報G_1とする）を導出し、第１勾配情報G_1及び重み変数Ｗに基づき、［数３］に示した算出方法で第１重み変数W_u（W_1）を算出してもよい。なお、第１重み変数W_1を算出するとき、例えば確率的勾配降下法以外の公知の方法を用いてもよい。

【００４５】

＜送受信手段：Ｓ１２０＞

次に、サーバ１０を介して第１重み変数W_1を、第１ユーザ端末２０ａから他のユーザ端末２０（以下、第２ユーザ端末２０ｂとする）に送信する（送受信手段Ｓ１２０）。このとき、例えば第１重み変数W_1を、複数のユーザ端末２０のうち第２ユーザ端末２０ｂのみに送信し、その他のユーザ端末２０には送信されない。

【００４６】

第１ユーザ端末２０ａの算出部２１は、各通信インターフェース２３、１３を介して、第１重み変数W_1をサーバ１０に送信する（第１手段Ｓ１２１）。サーバ１０の記憶部１２は、例えば取得した第１重み変数W_1を記憶する。

【００４７】

その後、サーバ１０の制御部１１は、各通信インターフェース１３、２３を介して、第１重み変数W_1を他のユーザ端末２０（以下、第２ユーザ端末２０ｂとする）に送信する（第２手段Ｓ１２２）。第２ユーザ端末２０ｂの記憶部２２は、例えば取得した第１重み変数W_1を記憶する。

【００４８】

例えば制御部１１は、複数のユーザ端末２０のうち、１つのユーザ端末２０を第２ユーザ端末２０ｂとして設定する。この場合、第２ユーザ端末２０ｂのユーザには、第１重み変数W_1が第１ユーザ端末２０ａによって算出されたことを秘匿することができる。

【００４９】

＜第２算出手段：Ｓ１３０＞

次に、第２ユーザ端末２０ｂにおいて、重み変数Ｗ（以下、第２重み変数W_2とする）を算出する（第２算出手段Ｓ１３０）。第２ユーザ端末２０ｂの算出部２１は、第２参照データと、第１重み変数W_1とを参照し、第２重み変数W_2を算出する。第１ユーザ端末２０ａの記憶部２２は、例えば算出した第２重み変数W_2を記憶する。

【００５０】

第２重み変数W_2を算出するとき、例えば上述した確率的勾配降下法を用いてもよい。この場合、第２ユーザ端末２０ｂの算出部２１は、第２参照データと、第１重み変数W_1とを参照して、［数２］に示した勾配情報Ｇ（以下、第２勾配情報G_2とする）を導出し、第２勾配情報G_2及び第１重み変数W_1に基づき、［数３］に示した算出方法で第２重み変数W_u（W_2）を算出してもよい。なお、第２重み変数W_2を算出するとき、例えば確率的勾配降下法以外の公知の方法を用いてもよい。

【００５１】

上述した動作を実施することで、本実施形態における学習システム１００の動作は終了する。なお、上述した動作は、２つのユーザ端末２０を用いた場合の最小限の動作を示しており、ｎつ（任意）のユーザ端末２０を用いる場合には、送受信手段Ｓ１２０と、第２算出手段Ｓ１３０とを複数回繰り返し行うことで、深層学習における再現性の最適化を行うことができる。また、１つのユーザ端末２０が複数回の重み変数Ｗを算出してもよく、この場合においても、送受信手段Ｓ１２０と、第２算出手段Ｓ１３０とを複数回繰り返し行うことで、深層学習における再現性の最適化を行うことができる。

【００５２】

次に、本実施形態におけるユーザ端末２０の構成の一例を説明する。なお、サーバ１０においても、ユーザ端末２０と同様の構成を備えることができるため、説明を省略する。

【００５３】

図４は、ユーザ端末２０の構成の一例を示す模式図である。ユーザ端末２０として、パーソナルコンピュータ（ＰＣ）等の電子機器が用いられる。ユーザ端末２０は、ＣＰＵ２

０１と、ＲＯＭ２０２と、ＲＡＭ２０３と、保存部２０４と、Ｉ／Ｆ２０５～２０７とを備える。各構成２０１～２０７は、内部バス２１０により接続され、筐体２１１内に格納される。

【００５４】

ＣＰＵ（Central Processing Unit）２０１は、ユーザ端末２０全体を制御する。ＲＯＭ（Read Only Memory）２０２は、ＣＰＵ２０１の動作コードを格納する。ＲＡＭ（Random Access Memory）２０３は、ＣＰＵ２０１の動作時に使用される作業領域である。保存部２０４は、記憶部２２を介して各種情報が保存される。保存部２０４としてデータ保存装置が用いられ、例えばＨＤＤ（Hard Disk Drive）、ＳＳＤ（solid state drive）等が用いられる。

【００５５】

Ｉ／Ｆ２０５は、公衆通信網３０等と接続するためのインターフェース部品であり、例えばＩ／Ｆ２０５を介してサーバ１０等との各種情報の送受信が行われる。

【００５６】

Ｉ／Ｆ２０６は、入力部分２０８との情報の送受信を行うためのインターフェース部品である。入力部分２０８として、例えばキーボードが用いられ、ユーザ端末２０のユーザ等は、入力部分２０８を介して、各種情報又はユーザ端末２０の制御コマンド等を入力できる。Ｉ／Ｆ２０７は、出力部分２０９との各種情報の送受信を行うためのインターフェース部品である。出力部分２０９は、保存部２０４に保存された各種情報、又はユーザ端末２０の処理状況等を出力できる。出力部分２０９として、例えばディスプレイが用いられる。なお、算出部２１、記憶部２２、及び通信インターフェース２３は、ＣＰＵ２０１が、ＲＡＭ２０３を作業領域として、保存部２０４等に保存されたプログラム（命令）を実行することにより実現される。

【００５７】

本実施形態によれば、送受信手段Ｓ１２０は、第１重み変数W_1を、第１ユーザ端末２０ａから第２ユーザ端末２０ｂに送信する。すなわち、各ユーザ端末２０で算出された重み変数Ｗを、サーバ１０を介したユーザ端末２０間で送受信し、深層学習における再現性の最適化を行う。このため、勾配情報Ｇをユーザ端末２０間で送受信した場合に比べて、送受信に必要となるデータ容量を大幅に縮小させることができる。これにより、ユーザ端末２０間におけるデータの送受信に費やす時間を削減でき、学習効率の向上を図ることが可能となる。

【００５８】

また、本実施形態によれば、送受信手段Ｓ１２０は、サーバ１０を介して第１重み変数W_1を、第１ユーザ端末２０ａから第２ユーザ端末２０ｂに送信する。すなわち、各ユーザ端末２０間において直接重み変数Ｗの送受信を行わない。このため、例えば第２ユーザ端末２０ｂに送信される第１重み変数W_1が、第１ユーザ端末２０ａにおいて算出されたことを他のユーザに対して秘匿することができる。これにより、ユーザ端末２０を保有するユーザに起因する情報の漏洩を抑制することが可能となる。

【００５９】

また、本実施形態によれば、送受信手段Ｓ１２０は、第１重み変数W_1を、第２ユーザ端末２０ｂのみに送信する。すなわち、各ユーザ端末２０において順番に重み変数Ｗが算出される手段を備える。このため、従来のような１つのユーザ端末において算出された勾配情報等を、複数のユーザ端末等に送信する手段に比べて、再現性の精度を飛躍的に向上させることができる。これにより、学習効率の向上を容易に図ることが可能となる。また、従来のような勾配情報等を複数のユーザ端末等に送信する必要が無いため、データの送受信に費やす時間をさらに削減することが可能となる。

【００６０】

また、本実施形態によれば、第１算出手段Ｓ１１０は、第１勾配情報G_1及び重み変数Ｗに基づく第１重み変数W_1を算出する。すなわち、ユーザ端末２０毎に勾配情報Ｇを導出し、重み変数Ｗを算出する。このため、勾配情報Ｇに含まれるユーザ端末２０毎に有す

る参照データを推定できる情報は、他のユーザ端末２０等に送信する必要が無い。これにより、各ユーザ端末２０の有ずる参照データの漏洩を抑制することが可能となる。

【００６１】

また、本実施形態によれば、送受信手段Ｓ１２０は、複数のユーザ端末２０のうち、１つのユーザ端末２０を第２ユーザ端末２０ｂとして、サーバ１０内において設定する。このため、重み変数Ｗが送受信される順番を、ユーザに知られないようにすることができる。これにより、ユーザ端末２０を保有するユーザに起因する情報の漏洩を容易に抑制することが可能となる。

【００６２】

（実施形態：学習システム１００の変形例）

次に、本実施形態における学習システム１００の変形例について説明する。上述した実施形態における学習システム１００の一例と、変形例との違いは、暗号化された重み変数W_Kが送受信される点である。なお、上述した内容と同様の構成等については、説明を省略する。

【００６３】

図５は、本実施形態における学習システム１００の変形例を示す模式図である。図５に示すように、各ユーザ端末２０は、暗号部２４を有する。なお、サーバ１０は、暗号部２４に該当する構成を有しない。

【００６４】

各ユーザ端末２０は、それぞれ等しい共通鍵暗号Ｋを有する。共通鍵暗号Ｋとして、例えばシーザ暗号、ＡＥＳ（Advanced Encryption Standard）、ＤＥＳ（Data Encryption Standard）等の公知のものが用いられる。暗号部２４は、共通鍵暗号Ｋを用いて重み変数Ｗの暗号化及び復号を行う。なお、共通鍵暗号方式は、例えば以下の多項式時間アルゴリズムから構成される。生成アルゴリズムＫｅＧｅｎ（１λ）は、セキュリティパラメータλを取り、共通鍵暗号Ｋを生成する。暗号化アルゴリズムEnc_K（ｍ）（又はＥｎｃ（Ｋ、ｍ））は、重み変数Ｗを暗号化する。復元アルゴリズムＤｅｃ（Ｋ、ｃ）は、暗号化された重み変数W_Kを復元する。例えばＣＰＡ（Ciphertext indistinguishability against chosen plaintext attacks）によって、暗号化された重み変数W_Kに含まれる情報の漏洩を防止することができる。

【００６５】

ユーザ端末２０は、算出された重み変数Ｗを暗号化し、サーバ１０を介して暗号化された重み変数W_Kを他のユーザ端末２０に送信する。このため、サーバ１０では、暗号化された重み変数W_Kを復号できず、重み変数Ｗを確認することができない。また、各ユーザ端末２０は、それぞれ等しい共通鍵暗号Ｋを有するため、何れのユーザ端末２０において暗号化された重み変数W_Kに対しても、復号することができる。

【００６６】

（実施形態：学習システム１００の動作の変形例）

次に、本実施形態における学習システム１００の動作の変形例について説明する。図６は、本実施形態における学習システム１００の動作の変形例を示すフローチャートである。本変形例によれば、学習システム１００は生成手段Ｓ１５０をさらに備え、第１算出手段Ｓ１１０は暗号化手段Ｓ１１２を有し、送受信手段Ｓ１２０は復号手段Ｓ１２３を有する。

【００６７】

＜生成手段：Ｓ１５０＞

先ず、共通鍵暗号Ｋを生成する（生成手段Ｓ１５０）。１つのユーザ端末２０（以下、第１ユーザ端末２０ａとする）の暗号部２４は、共通暗号鍵を生成する。暗号部２４は、例えばＳＳＬ／ＴＬＳ等の暗号化技術を利用して、生成した共通暗号鍵を直接他のユーザ端末２０（例えば第２ユーザ端末２０ｂ～第ｎユーザ端末２０ｎ）に送信する。他のユーザ端末２０のそれぞれの記憶部２２（２２ｂ～２２ｎ）は、取得した共通暗号鍵を記憶する。

【００６８】
このとき、サーバ１０を介さずにユーザ端末２０で共通鍵暗号Ｋの送受信を行うため、サーバ１０が共通鍵暗号Ｋを取得することを防止できる。また、各ユーザ端末２０が共通の共通鍵暗号Ｋを取得するため、１つのユーザ端末２０で暗号化された重み変数W_Kに対し、他のユーザ端末２０の何れにおいても復号でき、重み変数Ｗを取得することができる。
【００６９】
次に、上述した第１算出手段Ｓ１１０と同様に、第１ユーザ端末２０ａの算出部２１は、第１重み変数W_1を算出する。その後、第１ユーザ端末２０ａの暗号部２４は、共通鍵暗号Ｋを用いて、第１重み変数W_1を暗号化する（暗号化手段Ｓ１１２）。
【００７０】
次に、上述した送受信手段Ｓ１２０と同様に、第１ユーザ端末２０ａの算出部２１は、暗号化された第１重み変数W_{K1}をサーバ１０に送信する。サーバ１０の制御部１１は、暗号化された第１重み変数W_{K1}を第２ユーザ端末２０ｂに送信する。
【００７１】
その後、第２ユーザ端末２０ｂの暗号部２４は、共通鍵暗号Ｋを用いて、暗号化された第１重み変数W_{K1}を復号する（復号手段Ｓ１２３）。これにより、第２ユーザ端末２０ｂは、第１重み変数W_1を取得する。
【００７２】
次に、上述した第２算出手段Ｓ１３０と同様に、第２重み変数W_2を算出し、本実施形態における学習システム１００の動作は終了する。なお、上述した動作は、２つのユーザ端末２０を用いた場合の最小限の動作を示しており、ｎつ（任意）のユーザ端末２０を用いる場合には、第２算出手段Ｓ１３０のあと、暗号化手段Ｓ１１２～第２算出手段Ｓ１３０を複数回繰り返し行うことで、深層学習における再現性の最適化を行うことができる。また、１つのユーザ端末２０が複数回の重み変数Ｗを算出してもよく、この場合においても、暗号化手段Ｓ１１２～第２算出手段Ｓ１３０を複数回繰り返し行うことで、深層学習における再現性の最適化を行うことができる。
【００７３】
本変形例によれば、上述した実施形態と同様に、送受信手段Ｓ１２０は、第１重み変数W_1を、第１ユーザ端末２０ａから第２ユーザ端末２０ｂに送信する。すなわち、各ユーザ端末２０で算出された重み変数Ｗを、サーバ１０を介したユーザ端末２０間で送受信し、深層学習における再現性の最適化を行う。このため、勾配情報Ｇをユーザ端末２０間で送受信した場合に比べて、送受信に必要となるデータ容量を大幅に縮小させることができる。これにより、ユーザ端末２０間におけるデータの送受信に費やす時間を削減でき、学習効率の向上を図ることが可能となる。
【００７４】
また、本変形例によれば、上述した実施形態と同様に、送受信手段Ｓ１２０は、サーバ１０を介して第１重み変数W_1を、第１ユーザ端末２０ａから第２ユーザ端末２０ｂに送信する。すなわち、各ユーザ端末２０間において直接重み変数Ｗの送受信を行わない。このため、例えば第２ユーザ端末２０ｂに送信される第１重み変数W_1が、第１ユーザ端末２０ａにおいて算出されたことを他のユーザに対して秘匿することができる。これにより、ユーザ端末２０を保有するユーザに起因する情報の漏洩を抑制することが可能となる。
【００７５】
また、本変形例によれば、送受信手段Ｓ１２０は、暗号化された第１重み変数W_{K1}を、サーバ１０を介して第１ユーザ端末２０ａから第２ユーザ端末２０ｂに送信する。このため、サーバ１０では暗号化された第１重み変数W_{K1}を復元できず、第１重み変数W_1の内容を把握することができない。これにより、サーバ１０を保有する管理者等に起因する情報の漏洩を抑制することが可能となる。
【００７６】
本実施形態における学習方法は、上述した学習システム１００における第１算出手段Ｓ

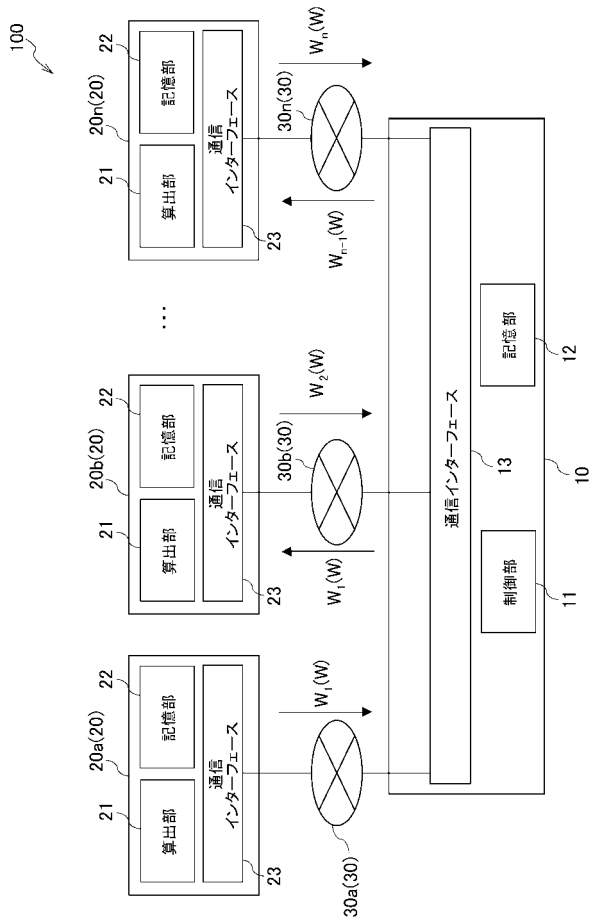
１１０と、送受信手段Ｓ１２０と、第２算出手段Ｓ１３０との代わりに、第１算出ステップと、送受信ステップと、第２算出ステップとを備えることで、上述した内容と同様に、勾配情報Ｇをユーザ端末２０間で送受信した場合に比べて、送受信に必要となるデータ容量を大幅に縮小させることができる。これにより、ユーザ端末２０間におけるデータの送受信に費やす時間を削減でき、学習効率の向上を図ることが可能となる。

【符号の説明】

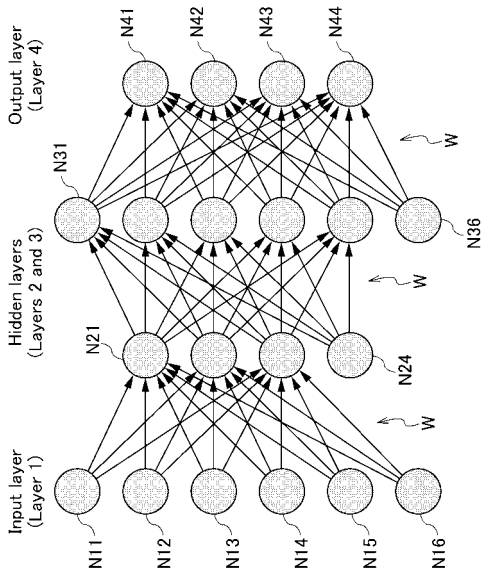
【００７７】

１０　：サーバ
１１　：制御部
１２　：記憶部
１３　：通信インターフェース
２０　：ユーザ端末
２１　：算出部
２２　：記憶部
２３　：通信インターフェース
２４　：暗号部
３０　：公衆通信網
１００　：学習システム
２０１　：ＣＰＵ
２０２　：ＲＯＭ
２０３　：ＲＡＭ
２０４　：保存部
２０５　：Ｉ／Ｆ
２０６　：Ｉ／Ｆ
２０７　：Ｉ／Ｆ
２０８　：入力部分
２０９　：出力部分
２１０　：内部バス
２１１　：筐体
Ｇ　：勾配情報
Ｋ　：共通鍵暗号
Ｎ　：ノード
Ｓ１１０　：第１算出手段
Ｓ１２０　：送受信手段
Ｓ１３０　：第２算出手段
Ｗ　：重み変数

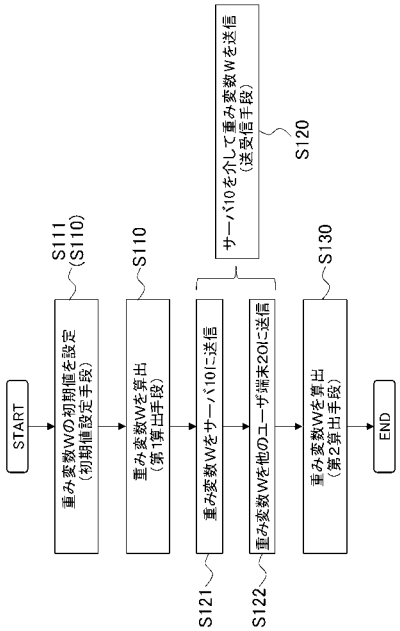
【図１】


100
20a(20)
20b(20)
20n(20)
21
算出部
22
記憶部
23
通信インターフェース
30a(30)
30b(30)
30n(30)
W1(W)
W2(W)
Wn(W)
Wn-1(W)
10
11
12
13
制御部
通信インターフェース

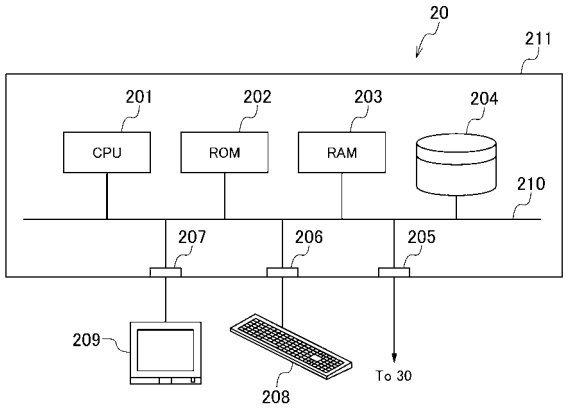
【図２】


Input layer
(Layer 1)
Hidden layers
(Layers 2 and 3)
Output layer
(Layer 4)
N11
N12
N13
N14
N15
N16
N21
N24
N31
N36
N41
N42
N43
N44
W

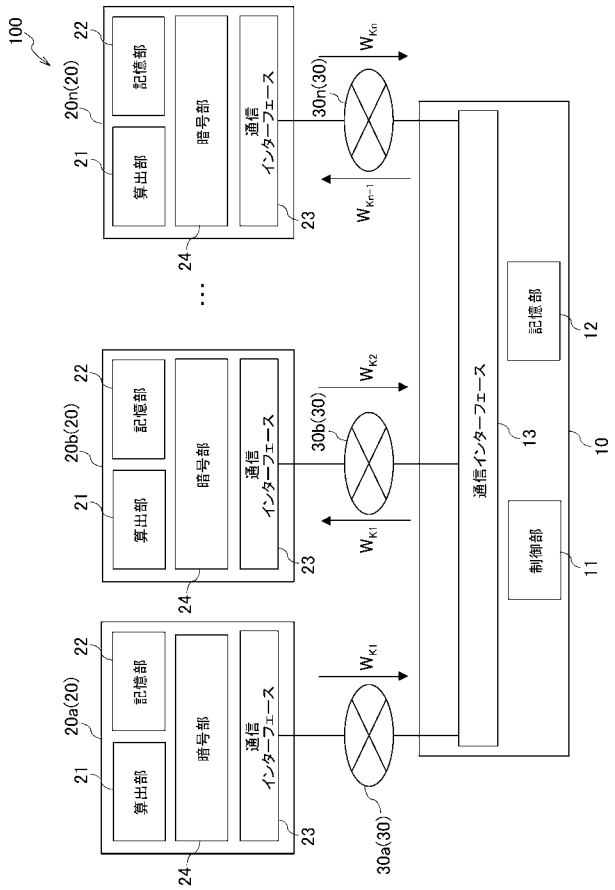
【図３】


START
重み変数Wの初期値を設定
（初期値設定手段）
S111
(S110)
重み変数Wを算出
（第1算出手段）
S110
重み変数Wをサーバ10に送信
S121
重み変数Wを他のユーザ端末20に送信
S122
サーバ10を介して重み変数Wを送信
（送受信手段）
S120
重み変数Wを算出
（第2算出手段）
S130
END

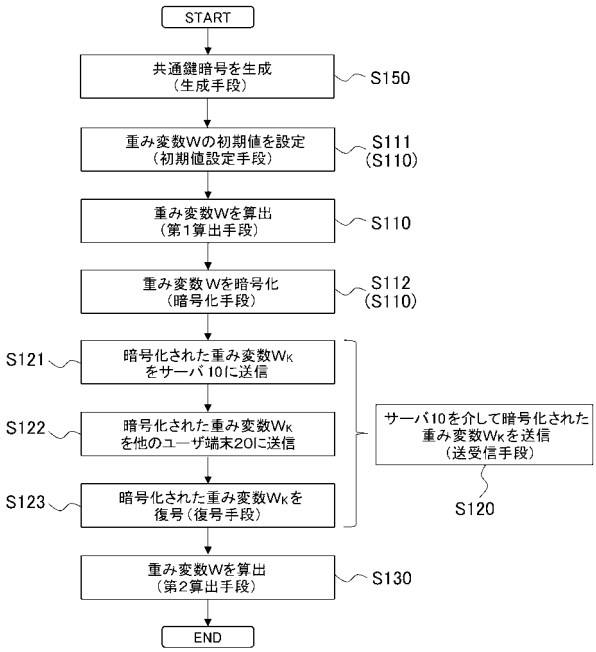
【図４】


20
211
201
CPU
202
ROM
203
RAM
204
210
207
206
205
209
208
To 30

【図５】


100
20n(20)
22
記憶部
21
算出部
暗号部
通信インターフェース
23
24
30n(30)
W_{Kn}
W_{Kn-1}
20b(20)
30b(30)
W_{K2}
W_{K1}
20a(20)
30a(30)
通信インターフェース
記憶部
12
13
10
制御部
11

【図６】


START
共通鍵暗号を生成
（生成手段）
S150
重み変数Wの初期値を設定
（初期値設定手段）
S111
(S110)
重み変数Wを算出
（第1算出手段）
S110
重み変数Wを暗号化
（暗号化手段）
S112
(S110)
S121
暗号化された重み変数W_K
をサーバ10に送信
S122
暗号化された重み変数W_K
を他のユーザ端末20に送信
S123
暗号化された重み変数W_Kを
復号（復号手段）
サーバ10を介して暗号化された
重み変数W_Kを送信
（送受信手段）
S120
重み変数Wを算出
（第2算出手段）
S130
END

フロントページの続き

（出願人による申告）平成２９年度、国立研究開発法人科学技術振興機構、戦略的創造研究推進事業に係る委託研究、産業技術力強化法第１９条の適用を受ける特許出願